UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

LUCAS ANTUNES TAMBARA

CARACTERIZAÇÃO DE CIRCUITOS PROGRAMÁVEIS E SISTEMAS EM CHIP SOB RADIAÇÃO

Porto Alegre
2013

LUCAS ANTUNES TAMBARA

CARACTERIZAÇÃO DE CIRCUITOS PROGRAMÁVEIS E SISTEMAS EM CHIP SOB RADIAÇÃO

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica, da Universidade Federal do Rio Grande do Sul, como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica.

Área de concentração: Engenharia de Computação - Micro e Nano Eletrônica

ORIENTADOR: Marcelo Soares Lubaszewski

Porto Alegre

2013

T154c Tambara, Lucas Antunes

Caracterização de circuitos programáveis e sistemas em chip sob radiação / Lucas Antunes Tambara. – 2013.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Escola de Engenharia. Programa de Pós-Graduação em Engenharia Elétrica. Porto Alegre, BR-RS, 2013.

Orientador: Prof. Dr. Marcelo Soares Lubaszewski

1. System-on-chips. 2. Field-Programmable Gate Arrays. 3. Tolerância a falhas. 4. Tolerância à radiação. 5. Efeitos da radiação. 6. Total Ionizing Dose. 7. Single Event Effects. I. Lubaszewski, Marcelo Soares, orient. II. Título

CDU-621(043)

LUCAS ANTUNES TAMBARA

CARACTERIZAÇÃO DE CIRCUITOS PROGRAMÁVEIS E SISTEMAS EM CHIP SOB RADIAÇÃO

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia Elétrica e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

Orientador: _____

Prof. Dr. Marcelo Soares Lubaszewski, UFRGS

Doutor pela Institut Nationale Polytechnique – Grenoble, França

Banca Examinadora:

Prof. Dr. Altamiro Amadeu Susin, UFRGS

Doutor pela Institut Nationale Polytechnique – Grenoble, França

Prof. Dr. Gilson Inacio Wirth, UFRGS

Doutor pela Universitaet Dortmund – Dortmund, Alemanha

Dr. Odair Lelis Gonçalez, IEAv

Doutor pela Universidade de São Paulo – São Paulo, Brasil

Coordenador do PPGEE: _____

Prof. Dr. João Manoel Gomes da Silva Júnior

Porto Alegre, Junho de 2013.

DEDICATÓRIA

Dedico este trabalho à minha noiva, Renata Borella Venturini, à minha mãe, Lúcia Regina Antunes Tambara, ao meu pai, Pedro Jorge Tadiello Tambara e à minha irmã Paula Antunes Tambara e à minha Mel, companhia sempre presente nos árduos dias de trabalho.

AGRADECIMENTOS

À minha noiva, Renata Borella Venturini, pelo apoio incondicional, carinho e compreensão, independente do momento. Eu não seria o homem que eu sou hoje sem ter você ao meu lado há onze anos.

Aos meus pais, Lúcia Regina Antunes Tambara e Pedro Jorge Tadiello Tambara, pela minha existência, formação, apoio incondicional e tudo mais que implica a relação entre pais e filhos.

À minha irmã, Paula Antunes Tambara, e ao meu cunhado, Albenir Querubini, pelo apoio e por me acolherem nos meus primeiros meses em Porto Alegre.

À UFRGS e ao Programa de Pós-Graduação em Engenharia Elétrica, por viabilizar a minha formação acadêmica. Ao CNPq, pela bolsa de mestrado concedida.

Ao meu orientador, Prof. Dr. Marcelo Lubaszewski, por me aceitar como aluno de mestrado e confiar em mim. Agradeço, em especial, à Prof.ª Dr.ª Fernanda Kastensmidt pelos ensinamentos, incentivo e confiança.

Aos demais professores e pesquisadores que contribuíram à realização deste trabalho, dentre eles o Prof. Dr. Tiago Balen, o Prof. Dr. Paolo Rech, o Dr. Odair Lelis Gonçalez e o Eng. Evaldo Junior.

Aos colegas de laboratório da sala 232 e demais, estejam eles em outras salas, cidades ou países, Eduardo, Felipe, Guilherme, Jimmy, Jorge, José Eduardo, José Rodrigo, Raul e William.

A todos meus amigos e pessoas importantes na minha vida.

RESUMO

Este trabalho consiste em um estudo acerca dos efeitos da radiação em circuitos programáveis e sistemas em chip, do inglês *System-on-Chip* (SoC), baseados em FPGAs (*Field-Programmable Gate Array*). Dentre os diversos efeitos que podem ensejar falhas nos circuitos integrados, destacam-se a ocorrência de *Single Event Effects* (SEEs), Efeitos Transitórios em tradução livre, e a Dose Total Ionizante, do inglês *Total Ionizing Dose* (TID). SEEs podem ocorrer em razão da incidência de nêutrons originários de interações de raios cósmicos com a atmosfera terrestre, íons pesados provenientes do espaço e prótons originários do Sol (vento solar) e dos cinturões de Van Allen. A Dose Total Ionizante diz respeito à exposição prolongada de um circuito integrado à radiação ionizante e cuja consequência é a alteração das características elétricas de partes do dispositivo em razão das cargas elétricas induzidas pela radiação e acumuladas nas interfaces dos semicondutores. Dentro desse contexto, este trabalho descreve em detalhes a caracterização do SoC-FPGA baseado em memória FLASH e de sinais mistos SmartFusion A2F200-FG484, da empresa Microsemi, quando exposto à radiação (SEEs e TID) através do uso da técnica de Redundância Diversificada visando a detecção de erros. Também, uma arquitetura que utiliza um esquema baseado em Redundância Modular Tripla e Diversificada é testada através da sua implementação no FPGA baseado em memória SRAM da família Spartan-6, modelo LX45, da empresa Xilinx, visando a detecção e correção de erros causados pela radiação (SEEs). Os resultados obtidos mostram que os diversos blocos funcionais que compõe SoC SmartFusion apresentam diferentes níveis de tolerância à radiação e que o uso das técnicas de Redundância Modular Tripla e Redundância Diversificada em conjunto mostrou-se extremamente eficiente no que se refere a tolerância a SEEs.

Palavras-chave: System-on-Chips (SoCs), Field-Programmable Gate Arrays (FPGAs), Tolerância à Falhas, Tolerância à Radiação, Efeitos da Radiação, Total Ionizing Dose (TID), Single Event Effects (SEEs).

ABSTRACT

This work consists in a study about the radiation effects in programmable circuits and System-on-Chips (SoCs) based on FPGAs (Field-Programmable Gate Arrays). Single Event Effects (SEEs) and Total Ionizing Dose (TID) are the two main effects caused by the radiation incidence, and both can imply in the occurrence of failures in integrated circuits. SEEs are due to the incidence of neutrons derived from the interaction of the cosmic rays with the terrestrial atmosphere, as well as heavy ions coming from the space and protons provided from the solar wind and the Van Allen belts. Total Ionizing Dose regards the prolonged exposure of an integrated circuit to the ionizing radiation, which deviates the standard electrical characteristics of the device due to radiation-induced electrical charges accumulated in the semiconductors' interfaces. In this context, this work aims to describe in details the characterization of Microsemi's mixed-signal SoC-FPGA SmartFusion A2F200-FG484 when exposed to radiation (SEEs and TID), using a Diverse Redundancy approach for error detection. As well, an architecture using a Diversified Triple Modular Redundancy scheme was tested (SEEs) through its implementation in a Xilinx's Spartan-6 LX45 FPGA, aiming error detection and correction. The results obtained show that several functional blocks from SmartFusion have different radiation tolerance levels and that the use of the Triple Modular Redundancy together with Diversified Redundancy proved to be extremely efficient in terms of SEEs tolerance.

Keywords: System-on-Chips (SoCs), Field-Programmable Gate Arrays (FPGAs), Fault tolerance, Radiation tolerance, Radiation Effects, Total Ionizing Dose (TID), Single Event Effects (SEEs).

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ABPS	Active Bipolar Prescaler
ACE	Analog Compute Engine
ADC	Analog-to-Digital Converter
AFE	Analog Front-End
AHB	Advanced High-performance Bus
APB	Advanced Peripheral Bus
ASIC	Application Specific Integrated Circuit
CLB	Configurable Logic Block
CMF	Common Mode Failure
CMOS	Complementary Metal-Oxide Semiconductor
COTS	Component Off-The-Shelf
DAC	Digital-to-Analog Converter
DDR	Design Diversity Redundancy
DMA	Direct Memory Access
DSP	Digital Signal Processor
DTMR	Diversity Triple Modular Redundancy
DUT	Device Under Test
DWC	Duplication With Comparison
EDAC	Error Detection And Correction
EMC	External Memory Controller
eNVM	Embedded Nonvolatile Memory
eSRAM	Embedded Synchronous Random-Access Memory
FFT	Fast Fourier Transform
FG	Floating Gate
FIFO	First In First Out
FPAA	Field-Programmable Analog Array
FPGA	Field-Programmable Gate Array

FSM	Finite State Machine
IEAv	Instituto de Estudos Avançados
I²C	Inter-Integrated Circuit
IP	Intelectual Property
ITAR	International Traffic in Arms Regulations
LET	Linear Energy Transfer
LUT	Look-up Table
MBU	Multiple Bit Upset
MOS	Metal-Oxide Semiconductor
MOSFET	Metal-Oxide Semiconductor Field-Effect Transistor
MPSoC	Multiprocessor System-on-Chip
MPU	Memory Protection Unit
MSS	Microcontroller Subsystem
NASA	National Aeronautics and Space Administration
NMR	N Modular Redundancy
PLL	Phase-Locked Loop
RC	Resistor-Capacitor
RMS	Root Main Square
SAR	Successive Approximation Register
SCB	Signal Conditioning Block
SE	Single Event
SEB	Single Event Burnout
SEE	Single Event Effect
SEGR	Single Event Gate Rupture
SEL	Single Event Latchup
SET	Single Event Transient
SEU	Single Event Upset
SRAM	Static Random-Access Memory
SoC	System-on-Chip
SPI	Serial Peripheral Interface
TID	Total Ionizing Dose
TMR	Triple Modular Redundancy
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus

VHDL Very High Speed Integrated Circuits Hardware Description Language

1 INTRODUÇÃO

A indústria de semicondutores apresentou uma rápida e notável evolução desde a produção do primeiro transistor na década de 1940. Com o transcorrer do tempo, os circuitos integrados tornaram-se mais complexos e densos, possibilitando a integração de diversos sistemas inteiros dentro de um mesmo chip. Esse aumento na capacidade de integração deve-se à tendência denominada de "escalonamento tecnológico" ou "miniaturização", cuja ocorrência proporcionou aos circuitos integrados grandes ganhos de desempenho através da redução das dimensões e da operação em voltagens mais baixas.

Exemplificando a evolução dos circuitos integrados no que diz respeito à sua redução em tamanho e em densidade com o passar do tempo, a Figura 01 demonstra que, entre os anos de 1970 e 2011, o comprimento da porta dos transistores de efeito de campo do tipo MOS (*Metal-Oxide-Semiconductor Field-Effetc Transistor* – MOSFET) sofreu uma redução de $10\,\mu m$ para 28 nm (círculos em amarelo, eixo y à direita) e o número de transistores por milímetro quadrado aumentou de duzentos para mais de dezenas de milhões (losangos, triângulo e quadrado, eixo y à esquerda).

A tendência de miniaturização dos circuitos integrados possibilitou a redução das dimensões das células de memória que, em conjunto com a redução das tensões de operação, contribuiu no aumento da densidade das memórias SRAM (*Static Random-Access Memory*) e FLASH, como é ilustrado na Figura 02. Nela, o gráfico à esquerda ilustra a redução da tensão de alimentação (eixo y à direita em verde) e da área ocupada por uma célula de memória SRAM (eixo y à esquerda em vermelho) com relação ao nó tecnológico (eixo x) em memórias SRAM. Também com relação à Figura 02, o gráfico à direita ilustra o aumento da densidade (eixo y) das memórias FLASH com o transcorrer dos anos (eixo x). Pode-se citar, ainda, o aumento no número de núcleos em um mesmo microprocessador. Segundo International Solid-state Circuits Conference (2011), no ano de 2001, os processadores possuíam em média dois núcleos e, no ano de 2011, o número de núcleos em um mesmo processador já era cinco vezes maior.

Por outro lado, tem-se que o escalonamento tecnológico tornou os circuitos integrados mais suscetíveis a falhas e aumentou a sensibilidade à variabilidade do processo de produção. As falhas podem ter origem em fatores diversos, tais como: erros de implementação, interações com o ambiente (interferências eletromagnéticas e incidência de radiação), perturbações na alimentação do dispositivo e efeitos de envelhecimento típicos de processos de fabricação modernos que podem afetar uniformemente uma região de modo a causar

múltiplas falhas (SRINIVASAN et al., 2008; HIARI et al., 2012). Outros efeitos provocados pela miniaturização consistem no surgimento do efeito de canal curto e o aumento das correntes de fuga (TAUR et al., 1997).

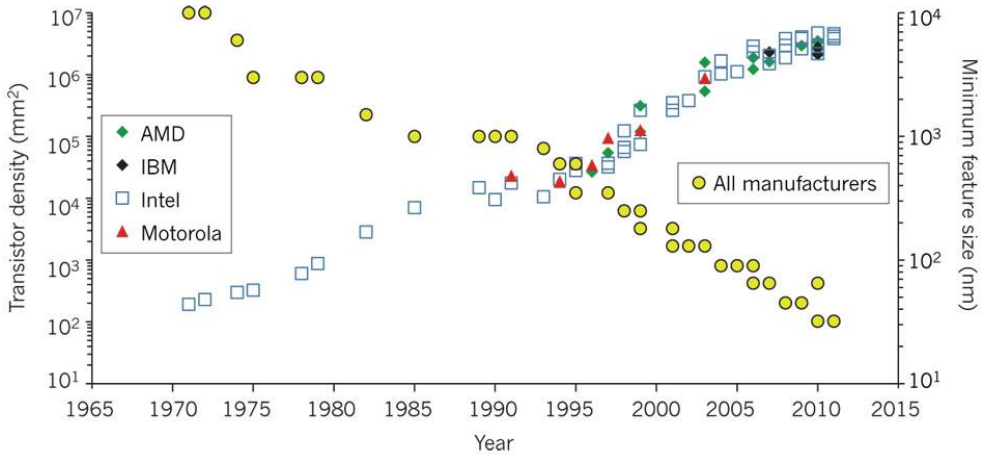

Figura 1 Evolução do comprimento da porta dos MOSFETs e da densidade de transistores em microprocessadores entre os anos de 1970 e 2011 (FERAIN, COLINGE, COLINGE, 2011).

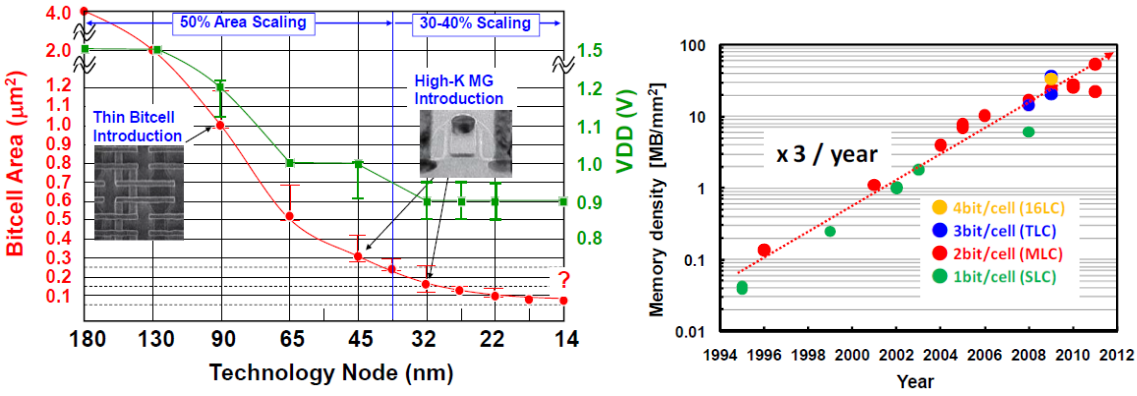

Figura 2 Ilustração da redução da tensão de alimentação e da área ocupada por uma célula de memória SRAM com relação ao nó tecnológico em memórias SRAM (gráfico à esquerda) e ilustração do aumento da densidade das memórias FLASH com o transcorrer dos anos (gráfico à direita) (INTERNATIONAL SOLID-STATE CIRCUITS CONFERENCE, 2011).

Dentre os efeitos que podem ensejar falhas nos circuitos integrados, destaca-se, hodiernamente, a incidência da radiação à medida que interfere na confiabilidade dos sistemas eletrônicos que atuam tanto no ambiente espacial quanto ao nível do mar. Pode-se citar, como exemplo de perturbações, a ocorrência de *Single Event Effects* (SEEs), Efeitos Transitórios em tradução livre, em razão da incidência de nêutrons originários de interações de raios cósmicos com a atmosfera terrestre, íons pesados provenientes do espaço e prótons

originários do Sol (vento solar) e dos cinturões de Van Allen (ZIEGLER et al., 1996; DODD et al., 2002; GASIOT, GIOT, ROCHE, 2006; ECOFFET, 2007).

Outro exemplo consiste no efeito conhecido por Dose Total Ionizante, do inglês *Total Ionizing Dose* (TID), o qual diz respeito à exposição prolongada de um circuito integrado à radiação ionizante e cuja consequência é a alteração das características elétricas de partes do dispositivo em razão das cargas elétricas acumuladas nas interfaces dos semicondutores e induzidas pela radiação.

Desse modo, a caracterização de circuitos integrados sob radiação têm se tornado uma etapa importante no processo de qualificação de componentes eletrônicos, especialmente em setores de aplicação que demandam um alto grau de confiabilidade como, por exemplo, o aeroespacial, o militar, o médico e o automotivo. Muitos experimentos têm sido realizados e os dados obtidos têm demonstrado como a confiabilidade das aplicações, principalmente as críticas, é seriamente afetada pela radiação. Como exemplo, em Dyer et al. (2004), tem-se que no ciclo solar de Outubro-Novembro de 2003, uma grande quantidade de SEEs foram observados em função da incidência de prótons solares e íons pesados em satélites. A radiação em altitudes aviônicas também é um grande perigo. Em altitudes de cerca de sessenta mil pés, nêutrons secundários provenientes da fragmentação de raios cósmicos são a mais importante contribuição à ocorrência de SEEs (TSAO, SILBERBERG, LETAW, 1984). Diversos experimentos de voos (NORMAND, 1996) têm demonstrado que partículas energéticas podem causar SEEs em componentes eletrônicos nessas altitudes. A radiação também é um problema no nível do mar, em especial em aplicações que requerem um alto grau de confiabilidade. Segundo Ziegler (2004), "*Efeitos Transitórios causados pela radiação são o limite primário no que diz respeito à confiabilidade da eletrônica digital. Este fenômeno é mais importante do que todas as outras causas que cercam a confiabilidade na computação juntas*".

Usualmente compostos por uma grande diversidade de blocos funcionais que podem, inclusive, ser de naturezas diferentes como processadores, memórias, matrizes programáveis e componentes analógicos, os atuais circuitos programáveis comerciais, como os *Field-Programmable Gate Arrays* (FPGAs), são verdadeiros sistemas em chip (*System-on-Chip* – SoC).

Os FPGAs e os SoCs podem ser programados através do uso de memórias SRAM, EEPROM ou FLASH. No caso da memória SRAM, uma memória volátil, torna-se necessária a adição de uma memória não volátil externa ao dispositivo FPGA para que a sua configuração (*bitstream*) seja armazenada e carregada sempre que ele é ligado. Nos

dispositivos baseados em memória FLASH, uma memória não volátil, a sua configuração permanece armazenada no próprio dispositivo, não sendo necessário carregá-la a partir de um componente externo. Essas diferenças refletem na susceptibilidade dos circuitos programáveis às falhas causadas pela incidência de radiação porquanto memórias FLASH são menos suscetíveis à ocorrência de SEEs (MICROSEMI, 2011b), ou seja, a sua configuração é mais difícil de ser alterada em razão da ocorrência de efeitos transitórios, o que não ocorre com os dispositivos baseados em memórias SRAM, as quais são mais sensíveis e exigem a reprogramação do dispositivo quando da ocorrência de um SEE.

No que se refere à tolerância a falhas em circuitos programáveis que operam em aplicações aviônicas e aeroespaciais, diversas técnicas de tolerância a falhas contra os efeitos da radiação podem ser implementadas em três níveis distintos durante o desenvolvimento de uma aplicação (FACCIO, 2007), quais sejam: em nível de processo, situação em que um determinado processo ou tecnologia de fabricação é alterado a fim de obter características de tolerância à radiação em um dispositivo, em nível de projeto, quando a estrutura ou lógica de um determinado circuito é alterada a fim de implementar técnicas de tolerância à TID ou SEEs em um dispositivo, e em nível de sistema, através da qual a implementação de um sistema é alterada a fim de obter tolerância a falhas.

Hodiernamente, há uma crescente motivação quanto ao uso de FPGAs comerciais (*Commercial Off-The-Shelf* – COTS) em aplicações que requerem um alto grau de confiabilidade com o objetivo de reduzir os custos do sistema final. Nesse contexto, o estudo e desenvolvimento de técnicas de proteção em nível de sistema são de grande importância, uma vez que, por padrão, nesses dispositivos não há nenhuma intervenção nas etapas de fabricação e projeto dos componentes que permita a inserção de recursos de tolerância a falhas.

Outra questão que torna importante o desenvolvimento de técnicas de tolerância a falhas em nível de sistema se refere às diversas regulamentações internacionais (*International Traffic in Arms Regulations* - ITAR) impostas pelos Estados Unidos no comércio de componentes eletrônicos. O ITAR considera que componentes eletrônicos tolerantes à radiação pode ser destinados à fabricação de artefatos bélicos e, por isso, eles não podem ser exportados pelos fabricantes de circuitos integrados dos Estados Unidos (COOK, 2010).

Dois dos grandes desafios acerca da caracterização de FGPAs e SoCs comerciais sob radiação consistem na acessibilidade reduzida dos blocos funcionais e nas restrições físicas impostas pelos componentes que, já em comercialização, tornam os procedimentos de caracterização mais complexos. É o que ocorre, exemplificativamente, em razão das

diferentes frequências de operação de blocos distintos de um FPGA ou SoC que dificultam a transferência de dados entre estes e os dados de diagnóstico entre o dispositivo e os equipamentos de aquisição de dados, os quais também possuem restrições de desempenho e de disponibilidade por parte da organização provedora do ambiente de caracterização.

Desse modo, este trabalho visa o desenvolvimento de uma metodologia de caracterização de circuitos programáveis comerciais sob radiação em nível de sistema. Para viabilizar a detecção e a mitigação de falhas causadas pela incidência de radiação nos circuitos programáveis comerciais utilizam-se, largamente, técnicas baseadas nos conceitos de redundância de hardware, de software e temporal.

Um dos métodos mais conhecidos é a Redundância Modular Tripla, do inglês *Triple Modular Redundancy* (TMR), que consiste na triplicação de um determinado circuito projetado onde as saídas das cópias são aplicadas a um votador de maioria. Porém, abordagens mais tradicionais como a replicação de componentes idênticos não estão imunes a falhas de modo comum (*Common Mode Failures* – CMFs) e falhas múltiplas. As CMFs são falhas que afetam mais de um módulo em um esquema redundante e ocorrem a um mesmo tempo, de um mesmo modo e, geralmente, devido a uma causa comum (AVIZIENIS et al., 1984).

Em contrapartida, quando as cópias de uma implementação em um sistema redundante são construídas com diferentes arquiteturas e/ou domínios (software, hardware digital ou hardware analógico), a probabilidade de falhas múltiplas afetarem diferentes blocos é reduzida uma vez que cada cópia pode apresentar diferentes níveis de tolerância associados às diferentes fontes e mecanismos de geração de falhas. Surge, desse modo, o conceito de Redundância Diversificada de Projeto em Sistemas Redundantes, do inglês *Design Diversity Redundancy* (DDR), em que uma mesma funcionalidade é desenvolvida utilizando-se implementações diferentes e/ou em domínios de projeto distintos, porém ainda funcionalmente idênticas.

Dentro desse contexto, esta dissertação almeja descrever em detalhes a caracterização do FPGA de sinais mistos SmartFusion A2F200-FG484, da empresa Microsemi (antiga Actel), quando expostos à radiação através do uso da técnica de Redundância Diversificada visando a detecção de erros. E de uma arquitetura que utiliza um esquema baseado em Redundância Modular Tripla e Diversificada implementada no FPGA da família Spartan-6, modelo LX45, da empresa Xilinx, visando à detecção e correção de erros.

Foram realizados três experimentos no FPGA SmartFusion, sendo dois de dose total ionizante, através do uso de radiação gama proveniente de uma bomba de Cobalto 60, e um de

Single Event Effects, através do uso de um acelerador para a geração de nêutrons. No FPGA Spartan-6 foi realizado um experimento de SEEs, também através de nêutrons.

Cumpre observar, ainda, que este trabalho está organizado da seguinte maneira: o Capítulo Dois descreve os efeitos da radiação em componentes eletrônicos; o Capítulo Três aborda o estado-da-arte no que diz respeito às técnicas de caracterização e tolerância a falhas baseadas em redundância para componentes comerciais; o Capítulo Quatro aborda os circuitos programáveis em FPGAs e SoCs sob uma visão genérica e os dispositivos utilizados nos estudos de caso deste trabalho; o Capítulo Cinco descreve a metodologia de caracterização de circuitos programáveis adotada para este trabalho, o primeiro estudo de caso, o qual objetivou a caracterização do SoC SmartFusion sob radiação, e o segundo estudo de caso, cujo objetivo foi analisar na prática o comportamento de uma arquitetura redundante e diversificada sob radiação; e, por fim, o Capítulo Seis apresenta as conclusões desta dissertação, as publicações decorrentes do trabalho realizado e os trabalho futuros a serem realizados.

2 EFEITOS DA RADIAÇÃO EM COMPONENTES ELETRÔNICOS

A pesquisa dos efeitos da radiação em dispositivos eletrônicos tornou-se altamente relevante para a comunidade científica de agências espaciais e de órgãos militares desde a perda do satélite de telecomunicações Telestar no ano de 1962 em razão da realização de um teste nuclear pelos Estados Unidos em alta altitude no oceano Pacífico. Sabe-se, desde então, que a radiação, seja natural ou induzida pelo homem, pode causar distúrbios no funcionamento de componentes eletrônicos (VELAZCO, FOUILLAT, REIS, 2007).

Analisado sob a ótica da radiação que contém, tem-se que o ambiente espacial é composto por partículas aprisionadas pela magnetosfera dos planetas, tais como os prótons, os elétrons e os íons pesados. Além disso, há também as partículas interplanetárias como os prótons, os íons pesados, as partículas primárias e secundárias presentes na atmosfera dos planetas. Não menos importante, a radiação em nível terrestre é composta por nêutrons provenientes da interação de raios cósmicos com partículas presentes na atmosfera terrestre.

As subseções a seguir apresentam uma revisão dos diferentes ambientes em que a radiação está presente, bem como o modo com que as diferentes partículas que podem compô-la afetam as funcionalidades dos componentes eletrônicos e como estes dispositivos são usualmente testados e caracterizados. A dose total ionizante e os efeitos transitórios são os dois efeitos da radiação abordados neste trabalho.

2.1 O AMBIENTE ESPACIAL E TERRESTRE NO ÂMBITO DA RADIAÇÃO

A radiação presente no espaço origina-se de três fontes diversas: do Sol, através dos ventos solares, dos raios cósmicos e dos Cinturões de Van Allen (CLAEYS, SIMOEN, 2002).

No que diz respeito à radiação proveniente do Sol, tem-se que a coroa solar – parte externa da atmosfera solar – emite um fluxo contínuo de prótons, elétrons e uma pequena quantidade de outros íons, o qual é comumente chamado de vento solar. Além desta fonte, o espaço interplanetário também contém partículas altamente energizadas chamadas de raios cósmicos, que podem atingir energias de até milhões de eV (CLAEYS, SIMOEN, 2002; BOUDENOT, 2007).

Durante o período de atividade máxima do ciclo solar, a atividade do Sol pode alterar o cenário espacial em razão do aumento do número e da intensidade das ejeções de massa coronal. Em contrapartida, durante o período de atividade mínima do ciclo solar, o fluxo de

raios cósmicos tende a aumentar uma vez que o campo magnético interplanetário encontra-se mais fraco nessa fase (EUROPEAN SPACE AGENCY, 1993).

Inserido no ambiente descrito, o campo magnético terrestre interatua com os ventos solares dando origem à cavidade denominada magnetosfera, ilustrada na Figura 3. A presença dos ventos solares dá à magnetosfera uma forma aproximadamente simétrica em relação ao campo magnético terrestre, estendendo-se por longas distâncias da superfície e abrindo-se nos pólos. No lado diurno, com o vento solar em condições moderadas, o plasma não penetra profundamente no campo magnético em razão da sua composição de partículas energizadas, de modo que 99% dessas partículas passam em torno da magnetosfera terrestre.

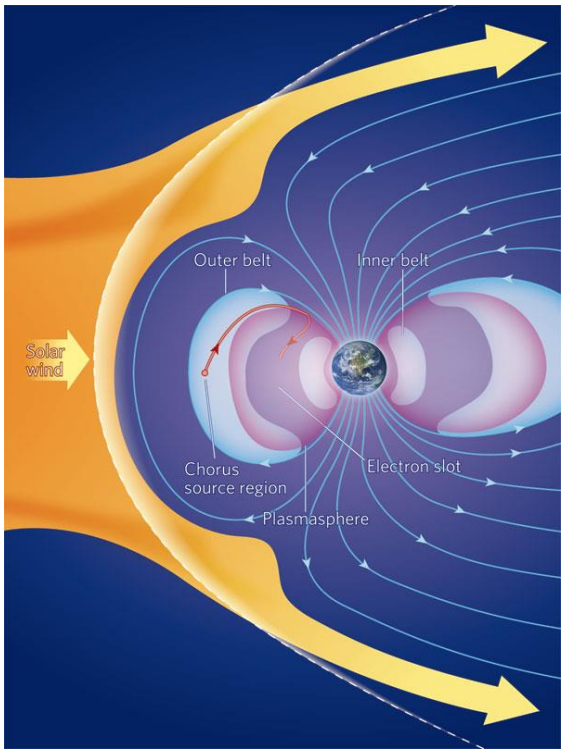

Figura 3 A magnetosfera terrestre gerada pelo vento solar e os cinturões de Van Allen (RODGER, CLILVERD, 2008).

O plasma presente na magnetosfera terrestre tem origem nos ventos solares e na ionosfera, localizando-se em baixas e médias latitudes no seu interior enquanto que, na parte mais externa, apresenta-se sob a forma de folhas de plasma. É através da sobreposição da plasmafera com as folhas de plasma que surgem os Cinturões de Van Allen, igualmente ilustrados pela Figura 3. Os elétrons presos nessas regiões possuem energias de até dezenas de MeV, enquanto que os prótons e os íons pesados presos possuem energias de até centenas de MeV (GUSSENHOVER, MULLEN, BRAUTIGAM, 1996).

A Terra é, então, atingida por partículas elementares e núcleos atômicos com grandes energias, os quais provêm dos ventos solares ou dos raios cósmicos e são constituídas, em grande parte, por prótons e íons pesados. À medida que ingressam na atmosfera terrestre, o fluxo de radiação cósmica é atenuado pela interação com átomos de oxigênio e de nitrogênio, por exemplo. Desse modo, um raio cósmico primário dificilmente atingirá o solo, pois irá colidir com várias partículas presentes no ar, geralmente a dezenas de quilômetros de altura, gerando muitas outras partículas de menor energia. Ocorre que, mesmo após o processo de atenuação, é possível que a interação dos raios cósmicos com a atmosfera gere uma cascata de partículas com energia suficiente para alcançar o nível do mar, como ilustrado Figura 4(a). Os resultados dessa cascata de raios cósmicos são, principalmente, íons pesados, prótons, elétrons, nêutrons e outras partículas elementares, como píons e múons.

Os nêutrons podem conter energias de até centenas de MeV e representam uma grande ameaça ao setor aviônico uma vez que o número máximo de partículas provenientes das cascatas geradas pelos raios cósmicos é encontrado justamente nas altitudes de voos, conforme se observa na Figura 4(b).

Mesmo ao nível do mar, existe a possibilidade de emissão de partículas provenientes de materiais radioativos. É o que se observa, exemplificativamente, com as partículas alfa que, altamente energizadas, são emitidas a partir de impurezas radioativas presentes em materiais utilizados no empacotamento de chips, como soldas ou compostos de moldes (BAUMANN, 2001). Estas partículas possuem energia cinética da ordem de alguns MeV.

A Tabela 1 descreve as faixas de energias das principais partículas de origem espacial em relação a sua fonte geradora.

Tabela 1 Faixas de energia das principais fontes de radiação espacial (ECOFFET, 2007)

Cinturões de radiação	Elétrons	1 eV – 10 MeV
	Prótons	1 keV – 500 MeV
Atividade solar	Prótons	1 keV – 500 MeV
	Íons	1 MeV – 10 MeV/n
Raios cósmicos	Prótons e Íons	Até 300 MeV/n

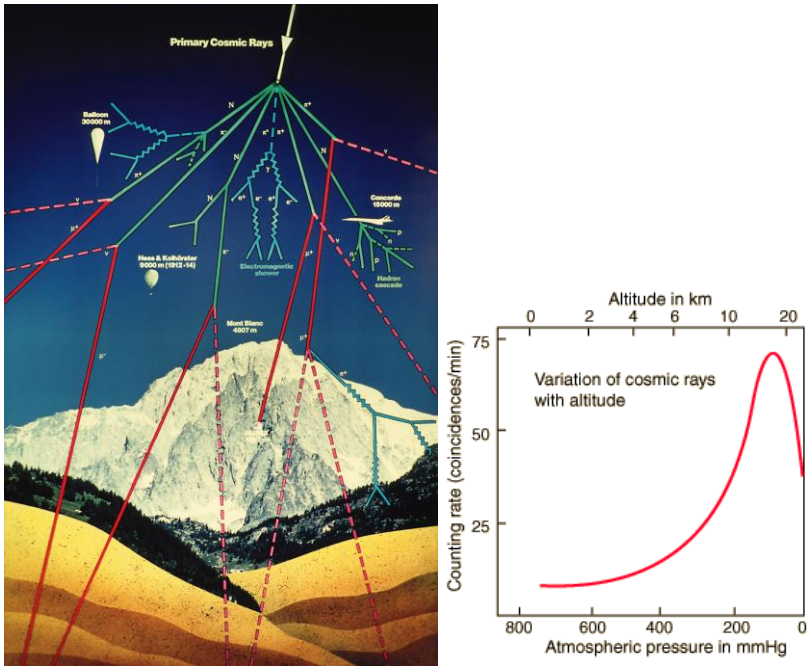

Figura 4 A imagem à esquerda ilustra um exemplo de cascata de partículas geradas devido a interação de um raio cósmico com a atmosfera terrestre (STEFAN, 2001). O gráfico à direita exemplifica que a cascata de partículas atinge o seu fluxo máximo em altitudes aviônicas (GEORGIA, 1999).

2.2 Efeito de Dose Total Ionizante

Os efeitos de dose total ionizante, do inglês *Total Ionizing Dose* (TID), decorrem da exposição de um componente eletrônico à radiação por determinado período de tempo (SCHRIMPF, 2007). Usualmente, tais efeitos são acumulativos e a sua intensidade está relacionada à intensidade e ao tempo de exposição do dispositivo à radiação incidente. Os primeiros estudos realizados acerca do acúmulo de cargas em óxidos de isolação devido à incidência da radiação ionizante foram divulgados em Snow et al. (1967).

A radiação ionizante, geralmente composta por elétrons provenientes de reações causadas pela incidência de partículas alfa, prótons e, também, pela exposição aos raios X e γ, pode causar significativas mudanças nos componentes eletrônicos, levando à degradação do dispositivo e, posteriormente, à sua falha funcional (SCHWANK et al., 2008). O aprisionamento de cargas no óxido e na interface Si/SiO_2 de um transistor é o principal evento que altera o comportamento nominal de um dispositivo eletrônico. Em um transistor, estas causas podem causar deslocamentos na tensão de limiar e o aumento das correntes de fuga.

Nas tecnologias em que os óxidos são mais finos, o aprisionamento de cargas ocorre com uma frequência menor, pois elas são rapidamente conduzidas para fora via tunelamento. Em contrapartida, óxidos muito finos são vulneráveis aos efeitos relacionados às correntes de fuga.

Os efeitos causados pela dose total ionizante em uma estrutura MOS serão descritos essencialmente através dos trabalhos de Oldham e MacLean (2003) e Schwank et al. (2008), que realizam uma revisão dos efeitos da radiação ionizante em óxidos de estruturas MOS. As figuras 5 e 6, apresentadas a seguir, não representam dados reais, apenas as principais características da resposta à radiação de um transistor MOS de tipo n tolerante a radiação.

O efeito comumente causado pela radiação em um transmissor MOS é ilustrado na Figura 5. A Figura 5(a) representa a operação normal de um transistor MOSFET em que a aplicação de uma tensão de porta apropriada leva à formação de um canal de condução entre a fonte e o dreno, o que faz com que a corrente flua entre esses dois terminais e o transistor seja ligado. A Figura 5(b), por sua vez, ilustra o efeito da radiação ionizante que consiste no aprisionamento de cargas no óxido de porta, o que causa um deslocamento na tensão de limiar do transistor, ou seja, uma mudança na tensão necessária que deve ser aplicada para ligar o transistor. Se este deslocamento for suficientemente grande, o dispositivo nunca mais será desligado, nem mesmo aplicando uma tensão de porta de zero volts.

Na prática, tem-se que o problema supracitado envolve diversos mecanismos físicos, em diferentes escalas de tempo e com diversas variáveis como, por exemplo, a temperatura. Por este motivo, a resposta de um dispositivo à radiação ionizante pode ser extremamente complexa.

A Figura 6 ilustra o esquemático de um diagrama de bandas de energia de uma estrutura MOS em que uma tensão de porta positiva é aplicada, tem-se, consequentemente, que os elétrons fluem em direção à porta e que as lacunas movem-se em direção ao substrato de silício. No esquemático, são enumerados diversos procedimentos envolvidos na resposta do dispositivo à radiação.

As partes mais sensíveis à radiação de uma estrutura MOS, no contexto de TID, são os óxidos isoladores (SCHWANK et al., 2008). Quando a radiação ionizante passa através do óxido de porta, pares elétron-lacuna são formados em razão da energia depositada pela partícula incidente, o que ocorre em um processo que dura alguns poucos picossegundos e que é responsável por quase todos os efeitos de dose total (SCHWANK et al., 2008).

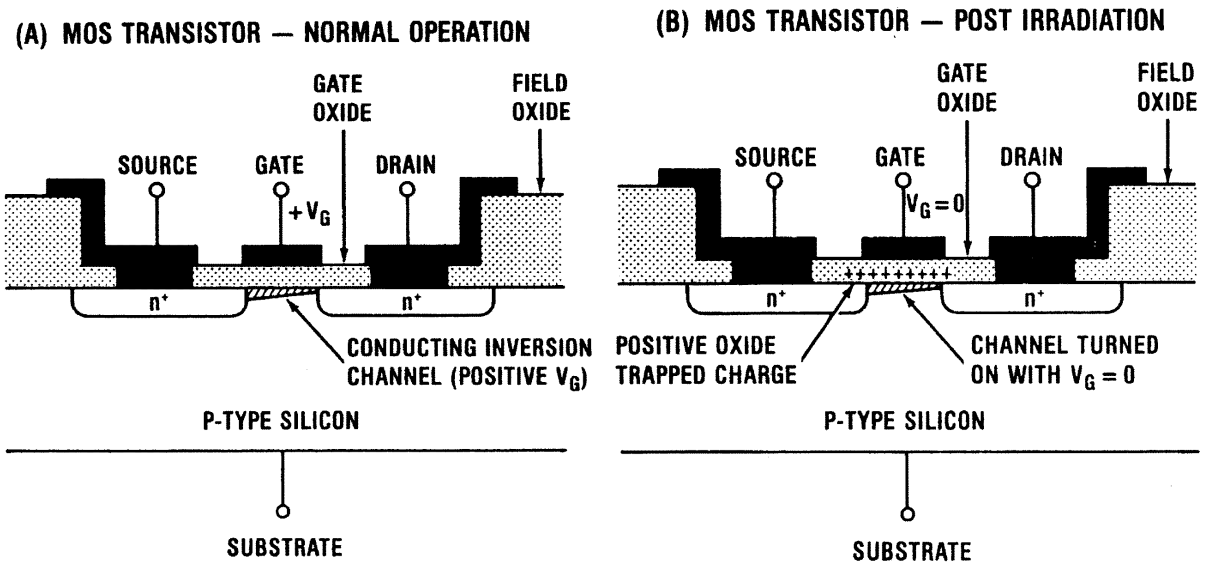

Figura 5 Esquemático de um transistor MOSFET do tipo n ilustrando o acúmulo de cargas no óxido de porta: (a) operação normal e (b) operação pós-irradiação (OLDHAM, MCLEAN, 2003).

No SiO_2, os elétrons são muito mais móveis do que as lacunas (HUGHES, 1973) e, por isso, são geralmente arrastados para fora do óxido. Entretanto, em um determinado momento desse transporte, uma fração dos pares elétron-lacuna irão sofrer um processo de recombinação que irá depender, principalmente, da energia e do tipo da partícula incidente. As lacunas são relativamente imóveis e permanecem próximas dos seus pontos de geração, onde causam um deslocamento negativo da tensão de limiar do transistor MOS (tipo n) atingido (OLDHAM, MCLEAN, 2003).

Os processos de geração de pares elétron-lacuna e de recombinação estão relacionados ao primeiro evento enumerado nas figuras 6 e 7.

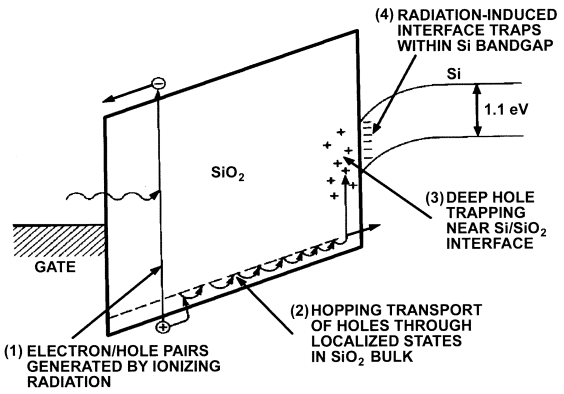

Figura 6 Diagrama de bandas de um estrutura MOS com uma tensão de porta positiva ilustrando o principal processo de aprisionamento de cargas provenientes da radiação ionizante (OLDHAM, MCLEAN, 2003).

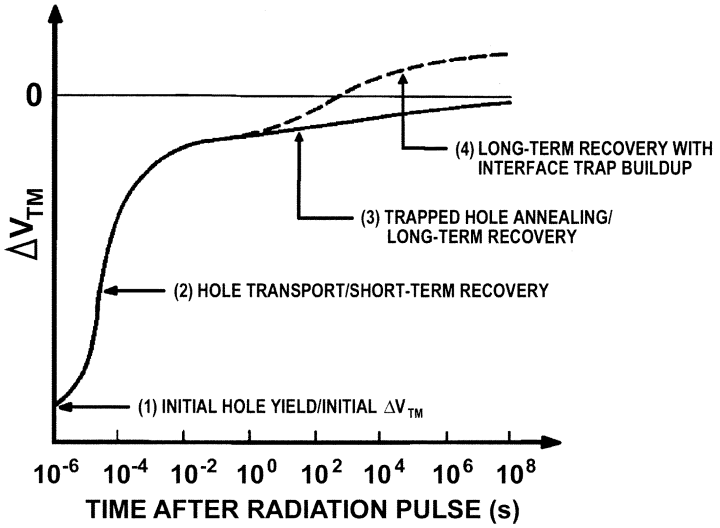

Figura 7 Gráfico da dependência do tempo versus a recuperação da tensão de limiar de um MOSFET do tipo n pós-irradiação em relação à Figura 13 (OLDHAM, MCLEAN, 2003).

O segundo processo descrito na Figura 6 consiste no transporte das lacunas para a interface Si / SiO_2, o que causa a recuperação na tensão de limiar ilustrada na Figura 7. Este é um processo relativo, ou seja, que ocorre ao longo de muitas décadas durante a operação do dispositivo e é muito sensível ao campo elétrico aplicado, à temperatura e à espessura do óxido (OLDHAM, MCLEAN, 2003).

Conforme ilustrado nas figuras 6 e 7, o terceiro processo ocorre quando as lacunas atingem a interface de silício. Nessa etapa, uma fração das lacunas transportadas fica em um estado de armadilha por um longo período, causando um deslocamento negativo na tensão de limiar que pode persistir por horas ou até anos. Contudo, até mesmo as lacunas aprisionadas e estáveis sofrem um processo de *annealing* gradual (OLDHAM, MCLEAN, 2003), em tradução livre, um processo de neutralização (ilustrado na Figura 7).

O quarto processo que envolve a resposta de uma estrutura MOS à radiação é a acumulação de armadilhas induzidas pela radiação na interface de Si / SiO_2 (OLDHAM, MCLEAN, 2003). Estas armadilhas são estados localizados com níveis de energia na banda proibida, do inglês *band-gap*, do silício (SCHWANK et al., 2008). A sua ocupação é determinada pelo nível de Fermi (ou pela tensão aplicada), o que dá origem a um deslocamento na tensão de limiar. A formação de armadilhas na interface é altamente dependente do processamento do óxido na etapa de fabricação do dispositivo e de outras variáveis, como o campo elétrico aplicado e a temperatura.

Com relação ao efeito de fuga de corrente, do inglês *current leakage*, tem-se que é decorrente do acúmulo de cargas na interface, o que faz com que resposta sub-limiar (*subthreshold*) do dispositivo seja alterada (SCHRIMPF, 2007), processo ilustrado no gráfico *Corrente de dreno X Tensão de porta* da Figura 8. Através da análise do gráfico, pode-se perceber que o acúmulo de cargas faz com que a inclinação da curva seja diminuída. Esta alteração torna-se crítica em transistores fabricados com tecnologias atuais que operam com valores reduzidos de tensão de alimentação e de limiar, pois mesmo com a aplicação de uma baixa tensão na porta do transistor, uma quantidade significativa de corrente pode fluir entre dreno e fonte, o que faz com que o consumo de potência estática do dispositivo aumente e, em alguns casos, impeça que o transistor seja até mesmo desligado.

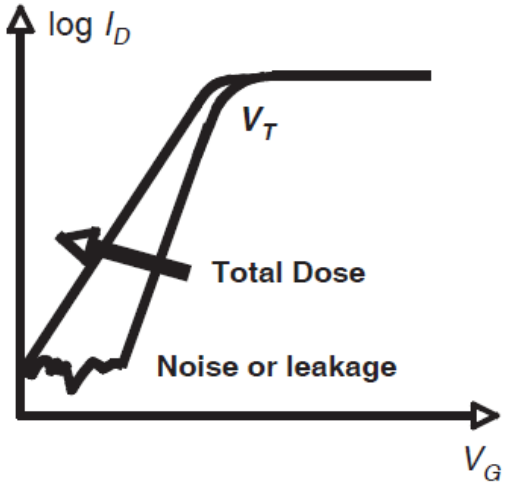

Figura 8 Gráfico *Corrente de dreno X Tensão de porta* para um MOSFET ilustrando a operação do dispositivo na região de sub-limiar (SCHRIMPF, 2007).

No que diz respeito à resposta de circuitos de sinais mistos à radiação, tem-se que o acúmulo de TID afeta os transistores MOS independentemente do seu domínio de aplicação, digital ou analógico, ocasionando efeitos similares em nível elétrico em ambos, mas distintos em nível de sistema. Um dos principais fatores responsáveis por esse comportamento está relacionado às diferenças existentes nas dimensões dos transistores que compõe os circuitos analógicos quando comparados com os digitais, visto que não acompanharam a tendência de escalonamento tecnológico em um mesmo ritmo que os circuitos digitais. Em decorrência disso, circuitos analógicos ainda apresentam camadas de óxido relativamente espessas que, em conjunto com as grandes dimensões dos seus transistores, resulta em uma maior vulnerabilidade a TID quando comparados com circuitos digitais baseados em processos de fabricação modernos.

Com relação ao comportamento de circuitos programáveis baseados em memórias FLASH e SRAM no contexto de TID, observa-se que ambos apresentam efeitos principais distintos, apesar de ambos os tipos de memórias serem baseados na estrutura MOS. No caso das memórias FLASH, a principal consequência é a perda de carga nas portas flutuantes (*floating gates*). Em memórias SRAM, a principal consequência é o aumento do atraso nos circuitos implementados, o que também ocorre em memórias FLASH.

É importante destacar que o escalonamento tecnológico proporcionou uma redução nas dimensões dos óxidos dos transistores de modo a reduzir significativamente os efeitos provocados pela dose total ionizante. Desse modo, os efeitos transientes passaram a ter um maior destaque na literatura.

2.3 EFEITOS DE FALHAS TRANSIENTES (*SINGLE EVENT EFFECTS*)

Em razão da expressiva evolução tecnológica nas últimas décadas, o número de componentes fabricados em um mesmo chip tem aumentado enquanto que o tamanho dos transistores continua a diminuir. À medida que tais avanços implicam em uma redução nas cargas armazenadas nos nós dos circuitos digitais, as cargas geradas por um SEE podem ser suficientemente grandes para perturbar um circuito. Por conta disso, os efeitos transitórios induzidos pela radiação tornam-se um dos mecanismos de falhas mais importantes em dispositivos eletrônicos modernos (WANG, AGRAWAL, 2008).

Os primeiros relatos acerca dos efeitos transitórios induzidos pela radiação datam da década de 1950 (ZIEGLER, LANFORD, 1979) e ocorrem quando uma partícula energizada (íons pesados, prótons, nêutrons, partículas alfa) presente no ambiente colide com um nó sensível de um circuito integrado. Dependendo de diversos fatores, tais como a energia que contém e o ângulo de incidência, a partícula incidente pode causar efeitos não observáveis, perturbações transitórias na operação do circuito, uma mudança de estado lógico ou até mesmo danos permanentes no dispositivo.

As regiões mais sensíveis de um transistor são geralmente as junções PN com polarizações invertidas (*reverse-biased*), pois o forte campo elétrico presente nessas regiões de depleção pode fazer com que ocorra uma coleta da carga proveniente da colisão de uma partícula energizada com o dispositivo. Além disso, a carga gerada pela colisão pode afetar localmente o campo elétrico da junção em razão da natureza altamente condutora do caminho que produziu e pela separação de carga que ocorre em função do campo elétrico da região de depleção (HSIEH, MURLEY, O'BRIEN, 1981), como ilustrado na Figura 9. Este efeito de

afunilamento pode aumentar a coleta de carga no nó atingido devido ao alargamento do campo elétrico, para além da junção PN e em direção ao substrato, de modo que a carga depositada a certa distância da junção possa ser coletada por meio do processo de deriva (DODD, MASSENGILL, 2003).

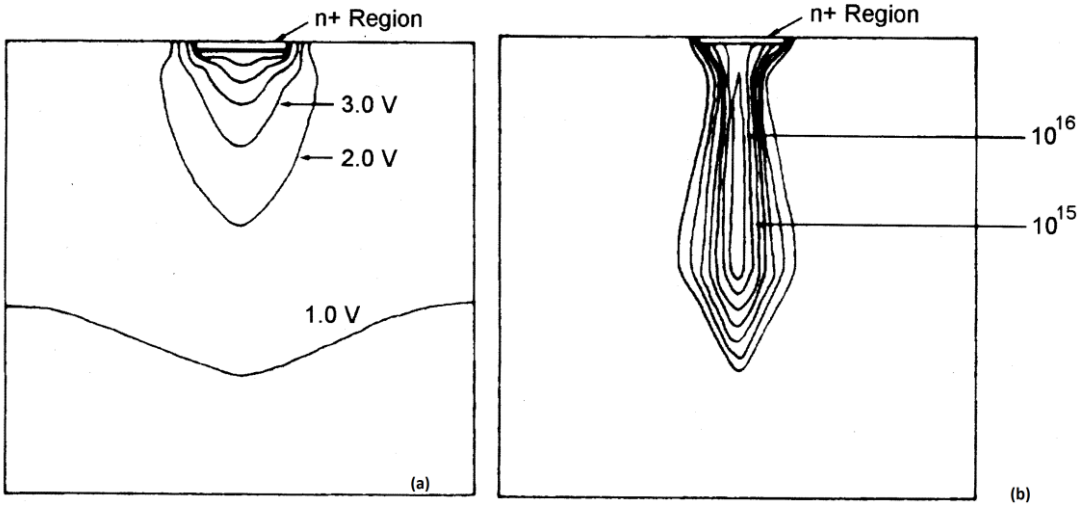

Figura 9 Ilustração do efeito de afunilamento em uma junção n^+/p de silício após a incidência de um íon: (a) potencial eletroestático e (b) concentração de elétrons (HSIEH, MURLEY, O'BRIEN, 1981).

A Figura 10 ilustra, exemplificativamente, o mecanismo básico de geração de um SEE devido à incidência de um íon pesado, o qual também pode ocorrer em razão da incidência de outras partículas radioativas. Na ilustração, pode-se observar a geração de pares elétron-lacuna e a posterior coleta de carga após a ocorrência do evento que, em nível elétrico, resulta em um pulso de corrente no dispositivo. O formato desse pulso decorre de dois mecanismos distintos que ocorrem após a passagem do íon incidente: inicialmente por deriva (*drift*) e, posteriormente, por difusão (*diffusion*) (BAUMANN, 2005a).

Existem dois métodos principais pelos quais a radiação ionizante libera carga em um dispositivo semicondutor, tratam-se da ionização direta pela partícula incidente e da ionização indireta por partículas secundárias geradas por colisões e reações nucleares entre a partícula incidente e o dispositivo atingido (DODD, MASSENGILL, 2003). Ambos os mecanismos podem levar ao mau funcionamento do dispositivo.

Na ionização direta, quando uma partícula energizada passa através de um material semicondutor, libera pares elétron-lacuna ao longo do seu caminho uma vez que perde energia e a transfere aos elétrons de valência. Na ionização indireta, quando um próton de alta energia

ou um nêutron penetra na estrutura cristalina do semicondutor, podem ocorrer diversas interações nucleares, é o caso das colisões elásticas que produzem o deslocamento de átomos de silício, da emissão de partículas alfa ou gama, da ejeção de núcleos secundários, bem como as reações de fissão, nas quais o núcleo atingido é divido em dois fragmentos (DODD, MASSENGILL, 2003). Qualquer produto dessas reações também pode depositar energia ao longo dos seus caminhos por ionização direta.

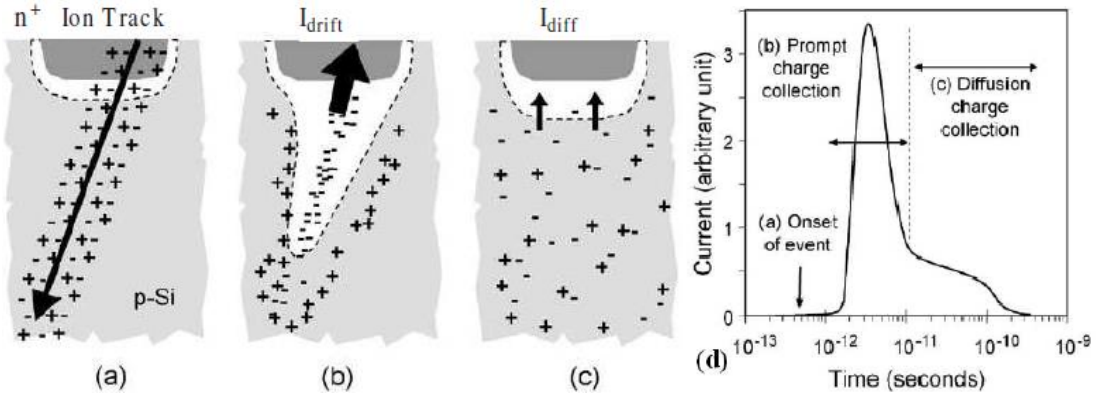

Figura 10 Ilustração da coleta de carga em uma junção PN de silício imediatamente após (a) a colisão de um íon pesado, (b) durante a coleta de carga por deriva, (c) durante a coleta de carga por difusão e em (d) é ilustrado o gráfico da corrente de junção induzida como função do tempo (WANG, AGRAWAL, 2008).

No que diz respeito às grandezas aplicáveis aos SEEs, tem-se importantes considerações a serem feitas. Isso porque a sensibilidade de um circuito a eventos singulares é definida em termos de área sensível total do dispositivo através da grandeza denominada de seção de choque, do inglês *cross-section* (σ), expressa em $cm^2 / dispositivo$ ou cm^2 / bit em função das equações (1) e (2) (VELAZCO, FAURE, 2007):

$$\sigma_{dispositivo} = \frac{número\,de\,SEEs\,obeservados\,durante\,o\,\exp erimento}{fluência\,do\,\exp erimento} \quad (1)$$

$$\sigma_{bit} = \frac{número\,de\,SEEs\,obeservados\,durante\,o\,\exp erimento}{(fluência\,do\,\exp erimento)\,x\,(número\,de\,bits)} \quad (2)$$

A fluência do experimento é dada pelo feixe de partículas incidentes por unidade de área (*partículas/cm²*). A taxa de fluência de um experimento é dada pelo feixe de partículas incidentes por unidade de área pelo tempo (*partículas/cm²/s*). Outra importante grandeza é a Transferência Linear de Energia, do inglês *Linear Energy Transfer* (LET), que corresponde à

perda de energia ionizante por unidade de comprimento de uma partícula à medida que ela passa através de um material ($MeV / mg / cm^2$) (BOUDENOT, 2007). É importante ressaltar que a grandeza LET é utilizada apenas no contexto de prótons e íons pesados uma vez que envolve ionização direta.

Os erros causados pela radiação podem ser destrutivos, chamados em inglês de *Single Event Hard Errors*, ou não destrutivos, chamados de erros transitórios, do inglês de *Soft Errors*, já exposto anteriormente.

No que diz respeito aos erros destrutivos, cumpre observar que não constituem o objeto deste trabalho, mas que englobam as seguintes espécies: *Single Event Burnout* (SEB), *Single Event Gate Rupture* (SEGR) e *Single Event Latchup* (SEL). Em qualquer um desses exemplos, a funcionalidade do dispositivo será permanentemente comprometida e, de um modo geral, as únicas soluções possíveis para esses problemas consistem na troca do dispositivo ou a sua submissão a um processo de neutralização (*annealing*), que pode ser efetivo ou não.

Quanto aos erros transitórios ou eventos únicos, termos usualmente utilizados como sinônimos pela literatura, tem-se que comprometem um valor lógico armazenado ou um sinal sem danificar o dispositivo. Os dois tipos de eventos transitórios de maior interesse para este trabalho consistem no *Single Event Upset* (SEU) e no *Single Event Transient* (SET).

Os SEUs diferenciam-se dos SETs em razão do seu caráter não transiente, pois são associados à inversão de bits de elementos de memória (DUZELLIER, BERGER, 2007). Nesse caso, a carga depositada por uma partícula que colide com o circuito integrado pode ser suficiente para inverter o estado de uma célula de memória. Segundo Wang e Agrawal (2008), a Agência Espacial Norte Americana (NASA) define os SEUs como os "*erros induzidos pela radiação em circuitos microeletrônicos são ocasionados quando partículas carregadas (normalmente provenientes dos cinturões de radiação ou de raios cósmicos) perdem energia, ionizando o meio pelo qual passam e deixando para trás um rastro de pares elétron-lacuna*".

As partes mais sensíveis de um circuito integrado a SEUs consistem nas junções PN de transistores desligados, mais especificamente, o dreno de transistores PMOS desligados e a região do canal de transistores NMOS desligados (DODD, SEXTON, 1995; DODD et al., 1996). Um dos elementos de memória mais utilizados nas últimas décadas é a célula de memória SRAM, de arquitetura tradicional composta por seis transistores. Quando uma partícula energética atinge uma das regiões sensíveis em célula de memória SRAM, o que é ilustrado na Figura 11, a carga coletada resulta em uma corrente transiente no transistor atingido. Essa tensão transiente pode ser similar a um pulso elétrico de escrita e pode levar a

memória a inverter o valor armazenado em sua célula. Esse mesmo raciocínio é válido também para uma célula de memória FLASH, cuja estrutura é ilustrada na Figura 12.

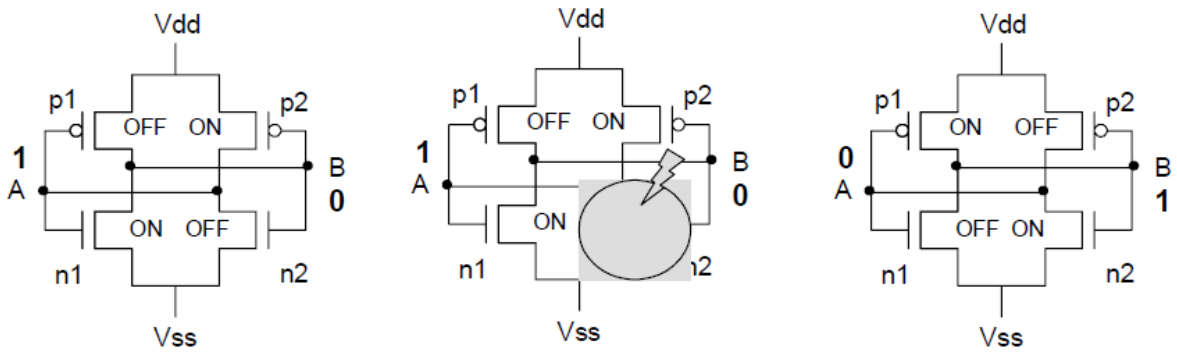

Figura 11 Exemplo da ocorrência de um SEU em uma célula de memória SRAM. Na primeira ilustração, da esquerda para a direita, é mostrado a célula com os seus valores corretos e, na terceira, é mostrado a configuração invertida da célula após a colisão de uma partícula no transistor inferior da direita (KASTENSMIDT, 2003).

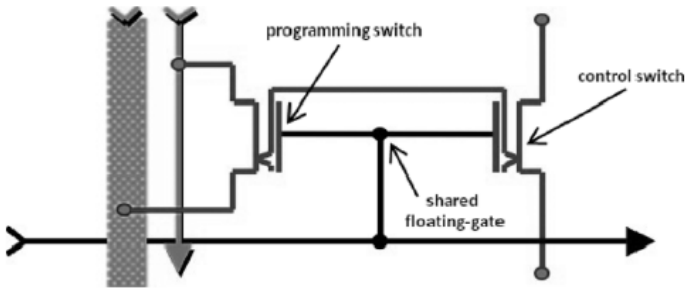

Figura 12 Estrutura de uma célula de memória FLASH onde são ilustradas as chaves de programação e de controle (BATTEZZATI et al., 2009).

Entretanto, a sensibilidade de uma célula SRAM à radiação depende de outros fatores além dos citados, como a energia da partícula incidente, a localização, o ângulo da colisão e o tempo de realimentação de célula (WEAVER et al., 1987). Com relação ao tempo de realimentação, tem-se que é o tempo necessário para a tensão do nó perturbado ser realimentada pelo par de inversores cruzados e, consequentemente, armazenar o valor errado no caso de uma colisão. Este tempo relaciona-se ao tempo de escrita da célula e pode ser visto, de uma maneira simples, como o atraso de um circuito Resistor-Capacitor (RC) no par inversor. Quanto menor for o atraso RC, mais rápida é a resposta da célula a uma tensão transiente e, consequentemente, mais sensível a SEUs (DODD, MASSENGILL, 2003).

Outra questão importante refere-se ao fato de que, à medida que as dimensões dos componentes eletrônicos diminuem constantemente em função do escalonamento tecnológico,

mais sensível se tornam as células de memória. Assim, é possível que uma única partícula incidente afete mais de um transistor ao mesmo tempo, posto que suas dimensões tornam-se menores que o caminho percorrido por uma partícula no dispositivo atingido. Desse modo, uma partícula pode corromper mais do que um único bit, gerando o evento chamado de *Multiple Bit Upset* (MBU) (DODD, MASSENGILL, 2003) e ilustrado na Figura 12.

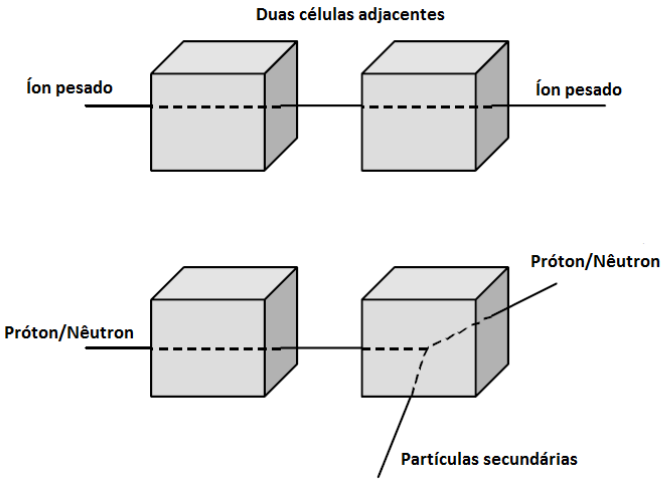

Figura 13 Exemplo da ocorrência de MBUs (KASTENSMIDT, 2003).

Em um nível maior de abstração, pode ser que o corromper de dados em razão de efeitos causados pela radiação seja catastrófico ou não, sendo possível que não ocorram erros observáveis quando levado em consideração o funcionamento de um sistema como um todo. Pode-se citar, exemplificativamente, o fato de que um dado corrompido torne-se obsoleto ou inutilizável com o passar do tempo e, desse modo, seja sobrescrito sem que nenhum sinal de um SEU permaneça. Entretanto, se os dados corrompidos pela radiação vierem a ser lidos e utilizados, é possível que diversos problemas ocorram, inclusive, o comprometimento integral de um sistema.

Atualmente, existem muitos códigos de correção de erro e estratégias de proteção que objetivam detectar e/ou corrigir inversões de bits para contornar SEUs. Contudo, a maioria dessas estratégias é desenvolvida para detectar ou corrigir apenas um bit errado por palavra de dado, o que possibilita que a ocorrência de MBUs torne-as ineficientes.

Os SEUs podem ser particularmente graves em FPGAs baseadas em memórias SRAM, posto que qualquer modificação na memória de configuração pode alterar o circuito implementado (BELLATO et al., 2004; VIOLANTE et al., 2007). Por outro lado, segundo Microsemi (2011b), FPGAs baseados em memórias FLASH são significativamente mais

tolerantes a SEUs que FPGAs baseados em memórias SRAM. Isso se dá porque a carga mínima necessária para perturbar o valor de uma célula de memória FLASH é significativamente maior do que em uma célula SRAM, ainda que os mecanismos de deposição de carga em um transistor sejam semelhantes em ambos os tipos de memórias

À medida que SETs podem ocorrer, assim como nos elementos de memória, os circuitos combinacionais não estão imunes aos erros provocados pela radiação. Um SET consiste em um pulso de corrente temporária gerada no nó de um circuito que pode ser propagado até um elemento de memória e armazenado, resultando em uma inversão de bit (SEU) (BAUMANN, 2005b). A Figura 14 ilustra a ocorrência de um SET.

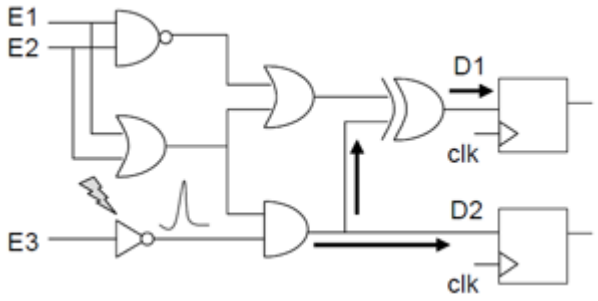

Figura 14 Exemplo da propagação de um SET em um bloco combinacional (KASTENSMIDT, 2003).

Em um circuito combinacional, em que a saída é baseada apenas na relação lógica entre as entradas, se uma carga proveniente de uma partícula radioativa incidente é coletada, será gerado na saída do circuito um pulso transitório, do termo inglês "*glitch"*. Se esse pulso for propagado para a entrada de uma memória, um *latch* ou um *flip-flop* durante uma borda sensível de sinal de relógio, o valor perturbado poderá ser capturado e armazenado, dando origem a uma inversão de bit. Um SET também pode gerar um atraso no valor correto na entrada de um *latch*, fazendo com que um valor errôneo seja armazenado. Entretanto, falhas de atraso são praticamente insignificantes em tecnologias modernas em razão do seu alto desempenho. Já em tecnologias mais antigas, é possível que um SET não seja propagado uma vez que pode não produzir uma alteração na saída do circuito e/ou ser rapidamente atenuado devido às largas capacitâncias e atrasos na propagação de sinais.

Apesar dos FPGAs baseados em memórias FLASH serem significativamente mais tolerantes a SEUs que FPGAs baseados em memórias SRAM (MICROSEMI, 2011b), eles não estão imunes à ocorrência de SETs em sua célula de programação básica, cuja estrutura é ilustrada na Figura 15. Considerando a estrutura ilustrada na Figura 15, é possível destacar

como exemplo três possíveis pontos sensíveis à ocorrência de SETs como consequência da incidência de uma partícula radioativa. *Effect 1*, o qual ocorre quando uma partícula atinge um nó sensível de uma porta lógica, provocando um pulso transiente (SET) que se propagará através da célula programável. *Effect 2*, o qual ocorre quando um pulso transiente se manifesta em uma lógica configurada para atuar como um *latch*. Nesse caso, devido ao caminho de realimentação existente na célula, o pulso transiente pode resultar em um SEU. E *Effect 3*, o qual ocorre quando uma partícula atinge um *floating gate*, o que pode gerar um pulso transiente.

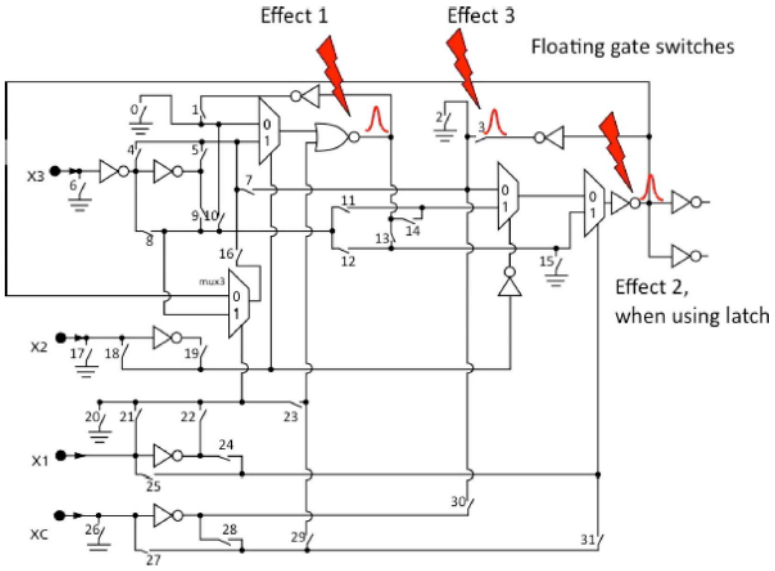

Figura 15 Estrura de uma célula de programação básica de um FPGA baseado em memória FLASH com possíveis pontos sensíveis à ocorrência de SETs em destaque (BATTEZZATI et al., 2009).

Como mencionado em Shivakuma (2002), uma mudança transiente no valor de um circuito lógico não irá afetar os resultados de uma computação ao menos que ela seja armazenada em um elemento de memória, logo, tal erro pode ser mascarado. Três tipos de mascaramento podem ocorrer, são eles: o lógico, o elétrico e que ocorre por janela de amostragem. O mascaramento lógico é o que ocorre quando o pulso resultante de uma partícula incidente atinge parte de uma lógica combinacional que não afeta a saída do circuito (ENTRENA et al., 2009), como ilustrado na Figura 16. Por sua vez, o mascaramento elétrico ocorre quando o pulso resultante da colisão de uma partícula é atenuado em amplitude ao longo do circuito combinacional até o ponto em que, ao chegar em um elemento de memória, ele não é capturado, como ilustrado na Figura 17. Por fim, tem-se que o mascaramento por

janela de amostragem ocorre quando o pulso resultante de um SET, mesmo invertendo temporariamente o nível lógico de um sinal em um circuito combinacional e até mesmo na entrada de um elemento de memória, ocorre fora do intervalo de tempo de captura do sinal, como ilustrado na Figura 18.

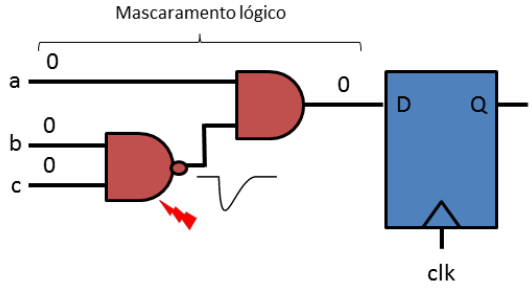

Figura 16 Exemplo de mascaramento lógico na propagação de um SET.

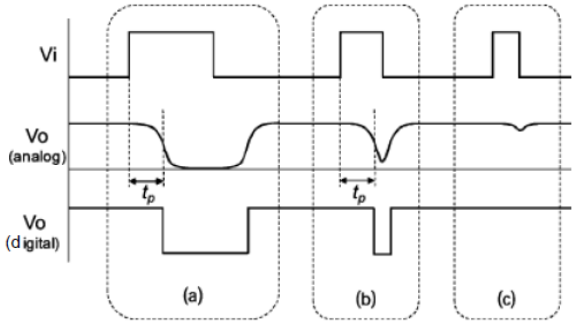

Figura 17 Exemplo de mascaramento elétrico na propagação de um SET (ENTRENA et al., 2009).

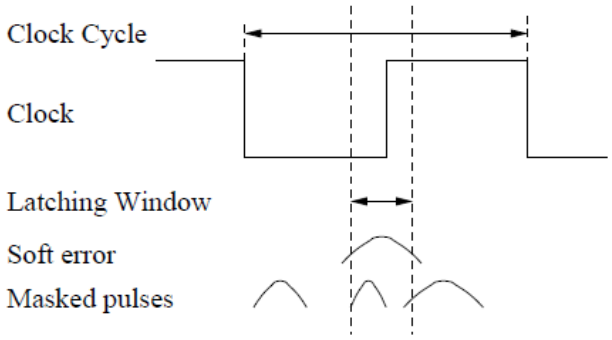

Figura 18 Exemplo de mascaramento por janela de amostragem na propagação de um SET (SHIVAKUMA, 2002).

É possível que os efeitos causados pelo mascaramento elétrico sejam atenuados em função do escalonamento tecnológico uma vez que transistores menores são mais rápidos e

podem ter um menor efeito sobre a atenuação do pulso gerado por um SET. Processadores com estágios de *pipeline* profundos que operam com grandes frequências de relógio podem reduzir os efeitos de mascaramento por janela de amostragem, uma vez que os seus *latches* irão operar com uma grande frequência, reduzindo assim as janelas de captura de um sinal. Desse modo, resta claro que a frequência de operação de um circuito tem um grande impacto na captura de SETs: quanto maior a frequência, maior é a probabilidade de haver elementos de memória corrompidos pela propagação de um pulso transiente.

De acordo com gráfico à esquerda da Figura 19, o impacto de SETs na taxa global de erros é significativamente menor em comparação aos SEUs para tecnologias anteriores as de 70 nm. Por outro lado, em tecnologias modernas cujo atraso de propagação é pequeno e a frequência de relógio é alta, um SET pode percorrer facilmente muitas portas lógicas, aumentando a probabilidade de ser capturado por um elemento de memória (BAUMANN, 2005b).

Segundo Borkar (2005), a cada geração tecnológica, espera-se um aumento de oito por cento na taxa de erro por bit de estado lógico. Isso se dá em razão da Lei de Moore, cujo enunciado dispõe que o número de bits de estado lógico dobra a cada geração tecnológica, conforme ilustrado pelo gráfico à direta da Figura 19. Exemplificativamente, é o que ocorre para uma tecnologia de 16 nm, cuja taxa de erros será quase cem vezes maior do que para uma tecnologia de 180 nm.

Imperioso notar que não foram encontrados dados acerca da relação entre a taxa de erros provocados pela radiação e as tecnologias de fabricação de memórias FLASH.

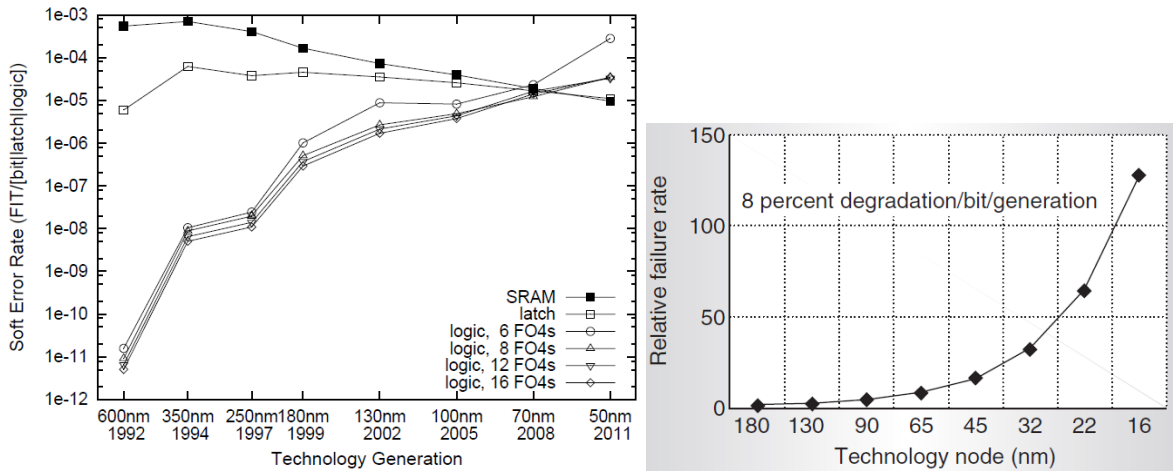

Figura 19 A esquerda, um gráfico que ilustra a taxa de erros suaves (*Soft Errors*) em circuitos individuais (SHIVAKUMA, 2002). A direita, um gráfico que ilustra a taxa relativa de erros suaves (*Soft Errors*) em um chip contendo elementos lógico e de memória (BORKAR, 2005).

3 TÉCNICAS DE CARACTERIZAÇÃO E TOLERÂNCIA BASEADA EM REDUNDÂNCIA DIVERSIFICADA PARA COMPONENTES COMERCIAIS

Os sistemas eletrônicos espaciais e aviônicos possuem uma ampla gama de componentes digitais e analógicos potencialmente sensíveis aos efeitos da radiação, motivo pelo qual devem ser qualificados ou, ao menos, protegidos para atuar em tais ambientes. É o que ocorre, por exemplo, nos projetos de aplicações espaciais em que os componentes tolerantes à radiação qualificados são largamente utilizados.

Ocorre que, atualmente, há uma forte tendência à utilização de componentes com qualificações militares ou de prateleira em sistemas aeroespaciais e aviônicos, os chamados *Components Off-The-Shelf* (COTS), cuja preferência decorre da necessidade de minimização dos custos e do tempo necessário para o desenvolvimento quando comparados aos dispositivos tolerantes à radiação (KATZ et al., 1997; O'BRYAN, LABEL, 2001). Tem-se, ainda, que o constante escalonamento tecnológico contribui para o aumento da sensibilidade dos circuitos integrados a algumas espécies de eventos causados pela radiação, como os *Single Event Effects*.

Em razão do cenário exposto e visando o desenvolvimento de um sistema com alto grau de confiabilidade, exsurge a necessidade de pesquisar técnicas de caracterização e de tolerância às falhas causadas pelos efeitos da radiação, tanto em nível terrestre quanto espacial. Trata-se, em verdade, de assegurar que o componente eletrônico mantenha-se operacional durante a sua vida útil mesmo na existência de SEEs, por exemplo.

Ainda que muitas técnicas tenham sido desenvolvidas nos últimos anos com a finalidade de evitar a ocorrência de SEUs e SETs, tem-se que a busca de soluções que visem a tolerância às falhas ainda constitui um desafio para as últimas gerações de semicondutores, especialmente devido ao aumento gradual na complexidade das novas arquiteturas (KASTENSMIDT, CARRO, REIS, 2006). Isso porque o desenvolvimento de técnicas de tolerância a falhas é fortemente associado ao dispositivo em que a técnica será embarcada, o que requer uma análise detalhada dos efeitos de uma inversão de bit na arquitetura em questão, entre outros. Nesse sentido, tem-se que, para cada tipo de circuito, há um conjunto de soluções que mais se adaptam a sua estrutura.

Assim, dependendo da fase de concepção de um circuito ou sistema, a técnica de tolerância a falhas contra os efeitos da radiação pode ser implementada em três níveis distintos durante o desenvolvimento de uma aplicação (FACCIO, 2007), quais sejam: em

nível de processo, situação em que um determinado processo ou tecnologia de fabricação é alterado a fim de dar características de tolerância à radiação à um dispositivo, em nível de projeto, quando a estrutura ou lógica de um determinado circuito é alterada a fim de implementar técnicas de tolerância à TID ou SEEs em um dispositivo, e em nível de sistema, através da qual a implementação de uma aplicação é alterada a fim de obter tolerância a falhas.

À medida que este trabalho faz uso de componentes comerciais (COTS), a técnica de tolerância a falhas que lhes é aplicável é a de nível de sistema, uma vez que, por padrão, não há nenhuma intervenção nas etapas de fabricação e projeto dos componentes que permita a inserção de recursos de tolerância a falhas.

As principais técnicas de tolerância a falhas para detecção e/ou mitigação de erros em nível de sistema são compostas por algum tipo de redundância e consistem em replicar componentes (redundância de hardware ou espacial) ou o tempo de execução de uma tarefa ou, ainda, amostragem de dados (redundância temporal) (ANGHEL, ALEXANDRESCU, NICOLAIDIS, 2000; KASTENSMIDT, CARRO, REIS, 2006). Frequentemente, as técnicas de tolerância implementam uma combinação de todos os tipos de redundância.

Ainda, as técnicas de tolerância a falhas são utilizadas tanto em módulos digitais quanto analógicos e podem abranger desde uma simples detecção de SEE até a votação e correção de uma inversão de bit.

Cumpre observar que também existem técnicas de tolerância a falhas que fazem uso de códigos de detecção e correção de erros. Contudo, tais métodos serão abordados apenas superficialmente porquanto este trabalho fundamenta-se exclusivamente no conceito de redundância.

3.1 TÉCNICAS DE REDUNDÂNCIA EM HARDWARE PARA DETECÇÃO DE FALHAS

As técnicas de detecção consistem, em grande parte, na duplicação de componentes em que a saída das cópias é enviada a um circuito comparador que identifica a existência ou não de uma falha, mas não a corrige, de modo que é possível detectar em qual componente ocorreu a falha. Este tipo de técnica, chamada pela literatura de *Duplication with Comparison* (DWC), Duplicação com Comparação em tradução livre, é bastante utilizada na caracterização de dispositivos e o seu uso permite a detectar erros em um componente e, consequentemente, estimar a sua susceptibilidade a falhas.

As técnicas que fazem uso da redundância temporal são usualmente utilizadas para detectar SETs em circuitos de lógica combinacional enquanto que, na redundância espacial, as técnicas são voltadas à identificação de SEUs em circuitos de lógica sequencial (ANGHEL, ALEXANDRESCU, NICOLAIDIS, 2000; KASTENSMIDT, CARRO, REIS, 2006). Exemplos do uso dessas técnicas podem ser encontrados em Nicolaidis (1999), Anghel et al. (2000) e Dupont et al. (2002).

No caso da redundância temporal, o objetivo da técnica é fazer uso das características do pulso transiente gerado pela colisão de uma partícula para comparar o sinal de saída de um circuito em dois momentos distintos. Ou seja, a saída de um circuito de lógica combinacional é capturada em dois momentos diferentes, nos quais a borda de um sinal de relógio é deslocada por um tempo d. Ao final, um comparador realiza a detecção de eventuais erros, podendo indicar a ocorrência de um pulso transiente e em qual cópia do circuito houve a manifestação, conforme ilustrado na Figura 20.

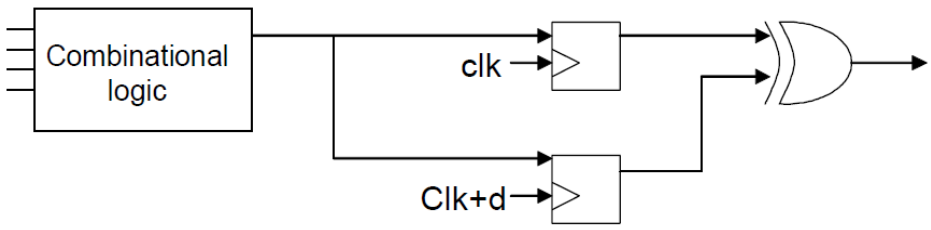

Figura 20 Exemplo de um esquema com redundância temporal para detecção de SETs em uma lógica combinacional (KASTENSMIDT, CARRO, REIS, 2006).

No caso da redundância de hardware, um esquema DWC pode ser usado para ambas lógicas combinacionais e sequenciais a fim de detectar SETs e SEUs, como ilustrado na Figura 21. Esta situação será posteriormente abordada com mais detalhes uma vez que constitui a base da técnica utilizada nesta dissertação.

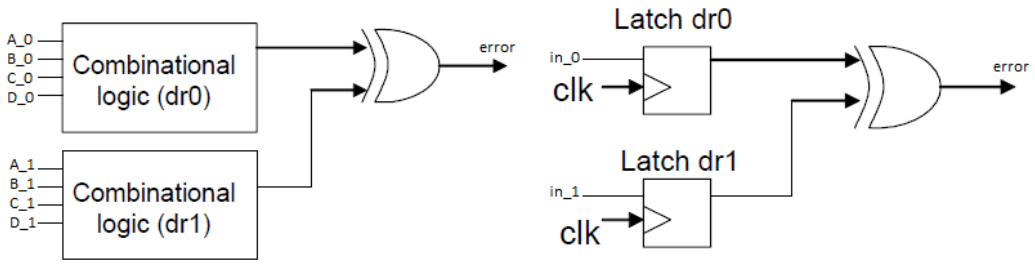

Figura 21 Exemplo de um esquema com redundância de hardware para detecção de (a) SET em uma lógica combinacional e (b) SEU em uma lógica sequencial (KASTENSMIDT, CARRO, REIS, 2006).

Outro exemplo de detecção de SEUs em circuitos com lógica sequencial consiste no uso de códigos de correção de erros como os bits de paridade (NICOLAIDIS, 2011), os quais são capazes de detectar inversões de bit simples ou múltiplos dependendo da implementação. Neste caso, o bit de paridade de um grupo de bits analisados é calculado e continuamente comparado com um novo bit de paridade calculado. Caso ocorra um SEU, é possível detectá-lo. Entretanto, para aplicações críticas, apenas a detecção da presença de uma falta não é suficiente, sendo também necessário garantir a operação correta do sistema na presença de uma falta. Um exemplo de esquema baseado em bits de paridade para detecção de SEUs é ilustrado na Figura 22.

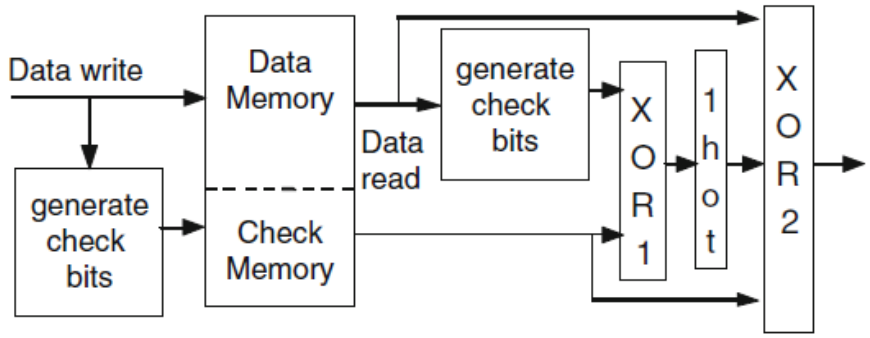

Figura 22 Exemplo de um esquema baseado em bits de paridade para detecção de SEUs em memórias (NICOLAIDIS, 2011).

3.2 TÉCNICAS DE REDUNDÂNCIA EM HARDWARE PARA MITIGAÇÃO E MASCARAMENTO DE FALHAS

Assim como nas técnicas de detecção, as técnicas de mitigação, em sua maioria, consistem na redundância espacial e/ou temporal de componentes, mais especificamente na sua triplicação. Com isso, as saídas de tais componentes são enviadas a um circuito comparador que, além de detectar a existências de uma falha, também deve corrigi-la.

As técnicas de mitigação que fazem uso da redundância espacial tendem a basear-se na *Triple Modular Redundancy* (TMR), a Redundância Modular Tripla em tradução livre. A técnica de TMR, mais popular entre as técnicas de redundância modular, consiste na triplicação de um determinado circuito projetado onde as saídas das cópias são aplicadas a um votador de maioria (*majority voter*) (KASTENSMIDT, CARRO, REIS, 2006;

KASTENSMIDT, REIS, 2007; NICOLAIDIS, 2011), como ilustrado na Figura 23. Na aplicação dessa técnica, se uma falha atingir um dos blocos triplicados, dois deles continuarão operando normalmente e o valor correto será escolhido pelo circuito votador. A desvantagem da utilização do TMR consiste no aumento da área ocupada pelo circuito, que será sempre maior de 200% em ralação a um circuito desprotegido.

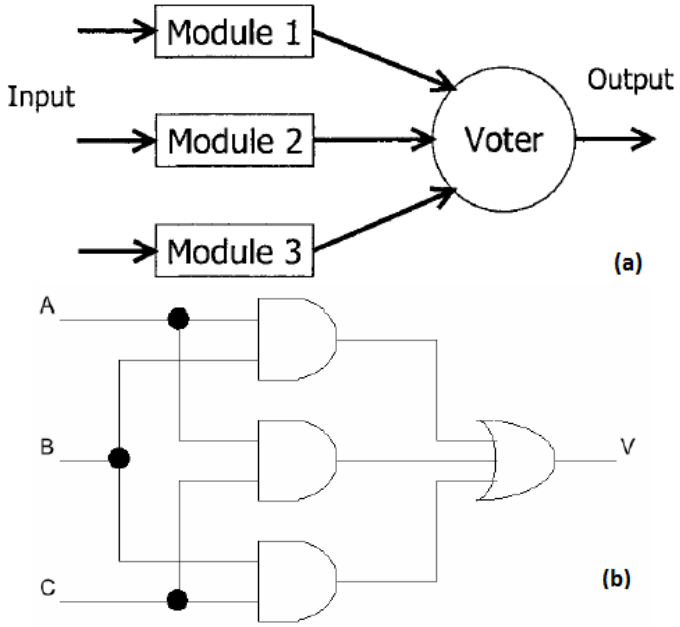

Figura 23 (a) Ilustração do conceito de TMR (GOLOUBEVA et al., 2006) e (b) esquemático de um votador de maioria (KASTENSMIDT, CARRO, REIS, 2006).

Um circuito com esquema TMR tradicional (três cópias idênticas) não está livre de apresentar falhas na sua saída. Isso porque é possível que ocorram falhas em blocos distintos de um mesmo esquema, de modo que a saída de cada um seja modificada e, consequentemente, o votador passe a escolher um valor incorreto uma vez que a maioria dos blocos estará com valores errôneos em suas saídas. Outra possibilidade consiste na ocorrência de um SEE no circuito votador, situação que pode ensejar a apresentação de um valor incorreto na saída do esquema de TMR. Há também a possibilidade de acumulação de erros (inversões de bits), o que exige a presença de um mecanismo extra para que seja corrigida a inversão de bit em cada cópia antes que um próximo SEU possa vir a ocorrer.

Para contornar a vulnerabilidade do votador e a acumulação de erros em um esquema com TMR, foi proposta a triplicação dos votadores e a adição de um caminho de reescrita para que fosse possível reescrever o valor correto nos elementos de memória do circuito (XILINX, 2001), conforme ilustra a Figura 24(a). Por se tratar da proteção de elementos de

memória (lógica sequencial), esta proposta é voltada apenas à proteção contra SEUs. Pode-se, contudo, proteger um circuito contra SETs através da triplicação dos blocos de lógica combinacional em conjunto com a proposta descrita para a proteção de SEUs, tal como ilustrado na Figura 24(b). Referida alteração implica em um grande aumento na área ocupada pelo circuito porquanto ambas as lógicas (sequencial e combinacional) são triplicadas, contudo, não se observam grandes perdas em questões de performance, mas apenas no tempo de propagação do votador.

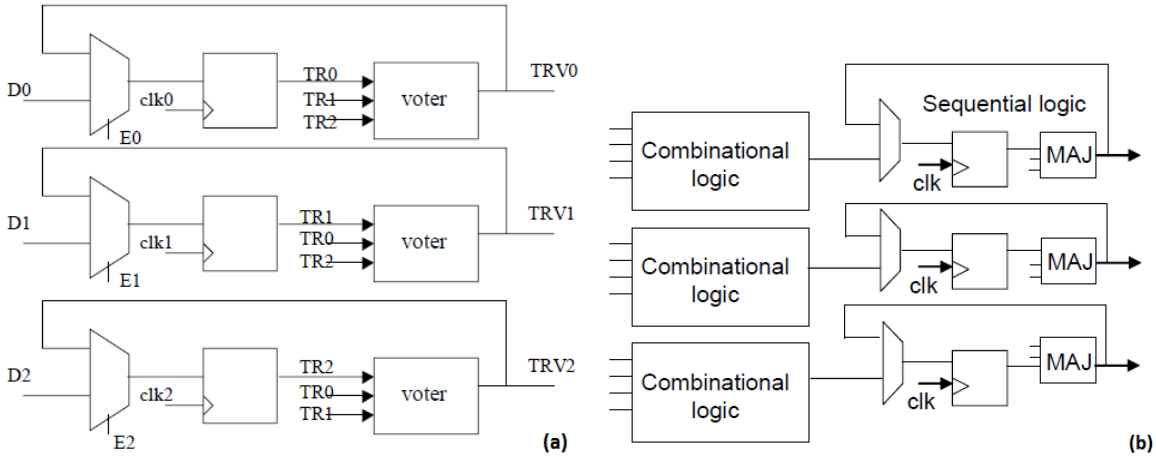

Figura 24 (a) TMR com votadores triplicados e células de memória com realimentação para proteção contra SEUs e (b) TMR com redundância completa para proteção contra SEUs e SETs (KASTENSMIDT, 2003). Ambos os esquemas são capazes de proteger os circuitos contra a acumulação de erros.

No que diz respeito à redundância temporal na mitigação de erros, tem-se que é usualmente voltada à proteção de circuitos com lógica combinacional porque permite votar a saída correta na presença de um SET, evento mais comum nesta espécie de circuito. E, assim como na redundância espacial, o uso de um esquema baseado na triplicação de blocos constitui a abordagem mais utilizada na redundância temporal. Referida técnica consiste no armazenamento do valor de saída de lógica combinacional em três momentos diferentes, em que a borda do sinal de relógio do segundo armazenamento é deslocado por um tempo *d* e a borda do sinal do terceiro armazenamento é deslocado por um tempo *2d*. Ao final da triplicação, um votador escolhe a saída correta. Este conceito é ilustrado na Figura 25.

As penalidades da redundância temporal em um circuito que implementa esta técnica estão relacionadas ao pequeno aumento de área em função dos *latches* extras e à redução de performance, que é dada por *clk+2d+tp* (Figura 25), onde *d* depende da duração do pulso transiente e *tp* é o atraso do votador de maioria (KASTENSMIDT, 2003).

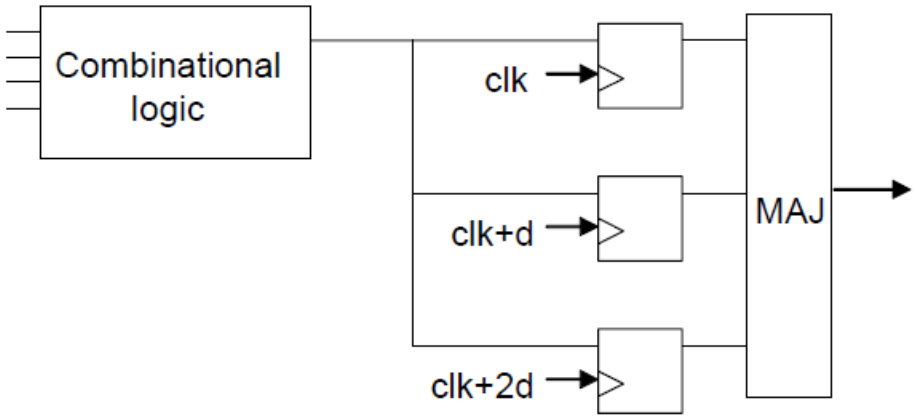

Figura 25 Ilustração do conceito de redundância temporal tripla (KASTENSMIDT, 2003).

Assim como a redundância espacial e temporal, os códigos de detecção de erros também são utilizados na mitigação de SEUs, sendo chamados de códigos de detecção e correção de erros, do inglês *Error Detection And Correction* (EDAC) (PETERSON, 1980). Este tipo de técnica é comumente utilizado para a proteção de sistemas contra SEUs, como em registradores, arquivos de registradores e memórias, sendo que a mais citada pela literatura é denominada de Código de Hamming (HOUGHTON, 1997).

A codificação de Hamming satisfaz a relação $2k \geq m + k + 1$, onde $m+k$ é o número total de bits na palavra codificada, m é o número de bits de informação na palavra original e k é o número de bits de checagem na palavra codificada. Seguindo esta equação, a codificação pode corrigir todos os erros únicos que ocorrerem em palavras de n bits e detectar erros duplos quando um bit de verificação geral de paridade é utilizado (KASTENSMIDT, CARRO, REIS, 2006).

Outro exemplo de técnica do tipo EDAC consiste na denominada Reed-Solomon (HOUGHTON, 1997), voltada à correção de erros múltiplos em aplicações de comunicação digital e armazenamento. Matematicamente, os códigos de Reed-Solomon são baseados na aritmética dos campos finitos. No caso da aplicação da técnica em memórias, cada palavra de dados é dividida em símbolos e cada uma representa uma codificação Reed-Solomon diferente. Por sua codificação e decodificação serem normalmente implementadas em softwares, os trabalhos encontrados na literatura não consideram seus efeitos na área e na performance de um hardware programável.

3.3 Técnicas de Redundância em Software para Detecção e Mitigação de Falhas

As técnicas de redundância em software consistem na replicação de programas, módulos, funções ou objetos com a finalidade de atingir um determinado nível de tolerância a falhas. Porém, a simples replicação de unidades idênticas de um software pode implicar na multiplicação de possíveis erros de projeto e de implementação de software (PULLUM, 2001). Nesse caso, se uma parte de um software é replicada e ocorrer uma falha em uma das cópias, tem-se que a mesma falha manifestar-se-á nas outras cópias, impossibilitando a detecção do problema, também. Em nível de hardware, muitos projetos não atentam a esta problemática, afirmando sua tolerância a falhas pelo simples uso de um esquema TMR tradicional (uso de cópias idênticas de um mesmo hardware).

De acordo com Pullum (2001), a aplicação do conceito de diversidade às réplicas é uma solução ao problema da replicação de possíveis falhas que possam vir a se manifestar nas cópias de um mesmo software. A abordagem básica para adicionar diversidade a um software redundante consiste na programação de uma mesma funcionalidade de maneiras diferentes, mas partindo de uma mesma especificação e atingindo o mesmo resultado final esperado. O resultado é a obtenção de componentes de software funcionalmente equivalentes e capazes de reduzir a probabilidade da ocorrência de falhas similares, de modo comum, coincidentes ou correlacionadas ao mesmo tempo. Assim como em um hardware redundante, um software redundante (e diversificado) requer um mecanismo de decisão capaz de votar o resultado correto dentre os fornecidos pelas réplicas, como um votador de maioria.

À medida que estruturada de diversas maneiras, as quais variam de acordo com hardware-base, a redundância em software permite que o sistema tenha todas as réplicas rodando em um mesmo componente de hardware, réplicas rodando em múltiplos componentes de hardware ou mesmo o mecanismo de decisão rodando em um componente de hardware e as réplicas em outro. Além disso, o software que é replicado pode variar de um programa inteiro a algumas poucas linhas de código (segmento de programa), ou seja, as abordagens a serem utilizadas na estruturação de um software redundante são baseadas principalmente nos recursos disponíveis e na aplicação específica.

3.4 TÉCNICA DE REDUNDÂNCIA DIVERSIFICADA PARA A CARACTERIZAÇÃO DE COMPONENTES COMERCIAIS E TOLERÂNCIA A FALHAS

Conforme exposto nas subseções anteriores, uma técnica que faz uso do conceito de redundância pode ter várias formas, podendo ser chamada, de um modo geral, de Redundância Modular *N*, do inglês *N Modular Redundancy* (NMR), onde *N* corresponde ao número de elementos redundantes idênticos presentes no sistema.

Ocorre que as técnicas de detecção e mitigação de falhas do tipo NMR são usualmente aplicadas em módulos distintos e não em um sistema em que os barramentos de dados, a comunicação, a memória, os módulos analógicos e digitais e os processadores sejam analisados em um mesmo contexto e ao mesmo tempo. Trabalhos em nível de sistema como (KUEN-JONG et al., 2010; GROSSO et al., 2010; CINARELLI et al., 2012) abordam um pouco essa questão. A análise simultânea de um sistema completo torna-se ainda mais relevante quando considerado um cenário de falhas múltiplas e os efeitos catastróficos de Falhas de Modo Comum, do inglês *Common Mode Failures* (CMFs).

As CMFs são falhas que afetam mais de um módulo em um esquema redundante, ocorrem a um mesmo tempo, de um mesmo modo e devido a uma causa comum (AVIZIENIS et al., 1984). As CMFs podem ocorrer em razão de erros de implementação, interações com o ambiente, interferência eletromagnética, perturbações na alimentação do dispositivo ou, em processos de fabricação modernos, pelos efeitos de envelhecimento onde os componentes podem ser afetados uniformemente em uma região de modo a causar múltiplas falhas de uma mesma maneira (SRINIVASAN et al., 2008; HIARI et al., 2012). A incidência de radiação, especialmente TID, pode afetar diferentes partes de um circuito ao mesmo tempo e de maneiras similares, podendo causar múltiplas falhas (BORGES et al., 2010a). Segundo Avizienis e Kelly (1984) e Mitra, Saxena e McCluskey (1999), os CMFs são bastante comuns em sistemas redundantes que utilizam as mesmas implementações e, consequentemente, muitas técnicas convencionais de redundância podem não apresentar resultados satisfatórios sob CMFs.

Por outro lado, se as cópias de uma implementação em um sistema redundante são construídas com diferentes arquiteturas e/ou níveis de abstração (software ou hardware), reduz-se a probabilidade de múltiplas falhas afetarem diferentes blocos uma vez que cada cópia pode apresentar diferentes níveis de tolerância associados às diferentes fontes e mecanismos de geração de falhas. Em razão disso, surge o conceito de Redundância

Diversificada de Projeto em Sistemas Redundantes, do inglês *Design Diversity Redundancy* (DDR), em que uma mesma funcionalidade é desenvolvida utilizando-se implementações diferentes e/ou em domínios de projetos distintos, porém, ainda funcionalmente idênticas. A Figura 26 ilustra um exemplo de redundância diversificada aplicada a um esquema com TMR em que cada um dos blocos é implementado de forma diferenciada em um mesmo domínio (digital via software e hardware) e em domínios diferentes (analógico e digital).

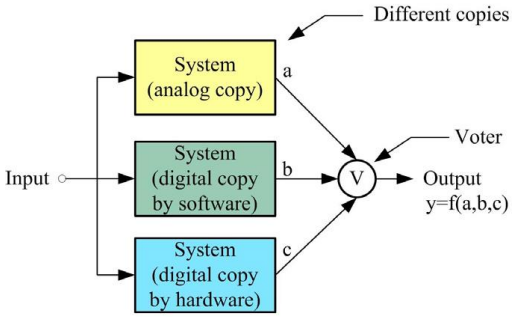

Figura 26 Exemplo da aplicação do conceito de diversidade de projeto em um esquema com TMR. Neste caso, cada bloco é implementado de maneira distinta (analógico, digital via software e digital via hardware) (BORGES et al., 2010a).

A diversidade de projeto foi proposta com a finalidade de proteger sistemas redundantes contra as falhas de um modo comum. Historicamente, o seu conceito foi proposto pela primeira vez em Elmendorf (1972) sob a denominação de "Programação em *N* Versões", do inglês "*N-Version Programming*", para aumentar a tolerância a falhas em projetos de softwares. O primeiro trabalho encontrado que abordou a implementação do conceito de diversidade de projeto foi Avizienis e Chen (1977), que aplicou a diversidade em nível de software. Em Avizienis e Kelly (1984), a diversidade de projeto foi definida como a geração independente de dois ou mais elementos implementados via hardware ou software para satisfazer uma determinada funcionalidade. A diversidade de projeto também foi adotada em Lala e Harper (1994) como uma técnica de prevenção contra falhas de modo comum. Segundo Riter (1995), o computador de voo dos aviões Boeing 777 implementam um esquema de redundância diversificada tripla através do uso de três processadores diferentes, sendo um da empresa Intel, um da AMD e outro da Motorola. Chau, Smith e Tai (2001) propuseram o uso da diversidade de projeto com a finalidade de aumentar a tolerância a falhas em barramentos de rede de aplicações aviônicas. Ashraf et al. (2011) utilizaram a redundância diversificada em FPGAs através de diferentes descrições de um mesmo hardware para aumentar a tolerância a falhas de projetos baseados em TMR. Além desses trabalhos citados

que, de um modo geral, descrevem aplicações do conceito de redundância diversificada, diversos trabalhos teóricos que objetivam a criação de métricas e realizam análises acerca da confiabilidade desta técnica já foram publicados (MITRA, SAXENA, MCCLUSKEY, 1999; 2001; 2002; 2004).

Trabalhos recentes (BORGES et al., 2010a; 2010b; HIARI, SADEH, RAWASHDEH, 2012) têm investigado a aplicação do conceito de redundância diversificada em componentes de sinais mistos para aumentar a confiabilidade dos projetos embarcados nesses dispositivos. Essa metodologia, referencia como TMR Diversificado, do inglês *Diversity* TMR (DTMR), propõe a utilização em paralelo de blocos funcionais implementados em domínios distintos, sendo um em software, um em hardware digital e o outro no domínio analógico.

Conforme exposto, os recentes avanços na indústria de semicondutores permitiram a integração de mais componentes em um mesmo chip. Assim, cada vez mais, a densidade dos FPGAs tem aumentado e um número maior de blocos funcionais periféricos, tanto digitais quanto analógicos, têm sido embarcados. Em razão dessa característica e da flexibilidade que esses dispositivos proporcionam, o uso da técnica de redundância diversificada torna-se uma opção atraente para a detecção de erros. Pode-se então afirmar que através do uso de um esquema de caracterização baseado em redundância diversificada é possível caracterizar simultaneamente diversas partes de um FPGA submetido à radiação. Isso porque através do seu uso é possível observar a distinção entre diferentes implementações, o que favorece a caracterização de mais de um componente paralelo. Tem-se como benefícios, ainda, a redução dos custos que envolvem a realização de uma caracterização como, por exemplo, da mão-de-obra necessária e do tempo utilizado, bem como os custos com o aluguel de um acelerador de partículas ou fonte de radiação ionizante para testes de SEEs e TID. Porém, esta abordagem nunca foi utilizada explicitamente na literatura com esse propósito.

4 CIRCUITOS PROGRAMÁVEIS EM FPGAS E SOCS

Os *Systems-on-Chip* (SoCs) programáveis são circuitos que apresentam um alto grau de integração e que geralmente contém diversos componentes necessários para o projeto de aplicações em hardware como, por exemplo, processadores, memórias e periféricos.

Usualmente, os SoCs são implementados de três modos diversos: no formato de circuitos integrados de aplicação específica (*Application Specific Integrated Circuit* – ASIC), através da descrição de um hardware em um *Field Programmable Gate Array* (FPGA) ou através da combinação de ambos. Muitas vezes, esses formatos são compostos pela união de blocos funcionais reutilizáveis denominados de Blocos de Propriedade Intelectual (*Intelectual Property Core* – IP *Core*) (GANSSLE, BARR, 2003).

Entre as principais vantagens no uso dos SoCs, sejam eles ASICs ou baseados em um FPGA, destacam-se a redução da área no projeto de um sistema, a minimização do gargalo de desempenho imposto pela comunicação entre diferentes blocos funcionais e a diminuição no tempo de desenvolvimento de um projeto (ZHU et al., 2002). Por outro lado, algumas dessas características podem ser consideradas pontos críticos no projeto de aplicações que exigem alto grau de confiabilidade como nos sistemas aviônicos e aeroespaciais, uma vez que podem transformar-se em pontos sensíveis a interferências internas e externas ao circuito, como as provocadas pela radiação espacial.

As subseções a seguir apresentam as características típicas de um SoC e os dois dispositivos físicos utilizados como objeto de experimentação deste trabalho no Capítulo 5.

4.1 ARQUITETURA TÍPICA DE UM SOC

A arquitetura de um SoC de sinais mistos genérico formado por diversos blocos funcionais como interfaces de comunicação, módulos de entrada e saída, um módulo de memória, um processador de sinais digitais (*Digital Signal Processor* – DSP), entre outros, pode ser observada na Figura 27. Uma rede de interconexões é responsável por conectar os diversos blocos funcionais entre si e também com os pinos de entrada e saída do componente.

Atualmente, diversos modelos de FPGAs e SoCs de sinais mistos são comercializados. Pode-se citar, como exemplo, o FPGA Zynq-7000, da empresa Xilinx, que possui, além de diversos periféricos, um processador de 32 bits e 800 MHz modelo ARM Cortex-A9 com dois núcleos, um FPGA baseado em memória SRAM e dois conversores analógico-digital de 12 bits (XILINX, 2012), o FPGA Cyclone V, da empresa Altera, que também possui, além de

diversos periféricos, um processador de 32 bits e 800 MHz modelo ARM Cortex-A9 com dois núcleos, um FPGA baseado em memória SRAM e dois conversores analógico-digital de 12 bits (ALTERA, 2012), o SoC PSoC, da empresa Cypress (CYPRESS, 2012); e o FPGA SmartFusion, da empresa Microsemi (MICROSEMI, 2012). Além dessas opções, há também tecnologias similares como as matrizes programáveis analógicas (*Field Programmable Analog Array* – FPAA) e os SoCs multiprocessados (*Multiprocessor SoC* – MPSoC).

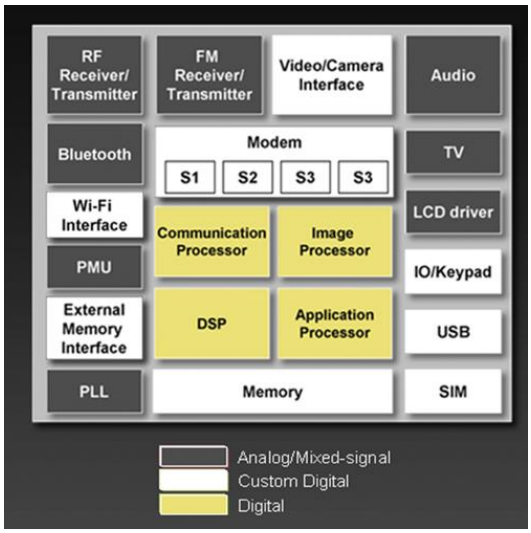

Figura 27 Arquitetura de um SoC genérico (CADENCE, 2010).

4.2 O FPGA SMARTFUSION, MODELO A2F200-FG484

Os primeiros manuais do FPGA SmartFusion datam de maio do ano de 2010, não sendo encontradas informações oficiais acerca do seu lançamento para o mercado de consumo. Segundo Microsemi (2012), o SmartFusion é o único FPGA que integra um processador ARM Cortex-M3 e blocos analógicos programáveis em um único componente.

Hodiernamente, é possível encontrar diversos FPGAs com características semelhantes ao SmartFusion, contudo, nenhum dos modelos disponíveis é concebido a partir de um processo de fabricação baseado em células de memórias do tipo FLASH (MICROSEMI, 2011a).

Em FPGAs, a tecnologia FLASH, com a sua estrutura de armazenamento não volátil, é uma alternativa à tecnologia SRAM, amplamente utilizada apesar de volátil. A célula de memória FLASH tem como principal característica a sua porta flutuante, do inglês *Floating Gate* (FG), localizada entre a porta de controle e a estrutura MOSFET e estando envolto em um material dielétrico. Essa estrutura é ilustrada na Figura 28.

O valor de um bit em uma célula de memória FLASH é armazenado como uma carga no *floating gate*. Por exemplo, uma porta com carga representa um valor lógico zero para uma célula de memória FLASH baseada em uma estrutura NOR. Escrever ou apagar um valor lógico em uma célula requer uma alta tensão e alguns milissegundos de tempo para adicionar ou dissipar uma carga do *floating gate*.

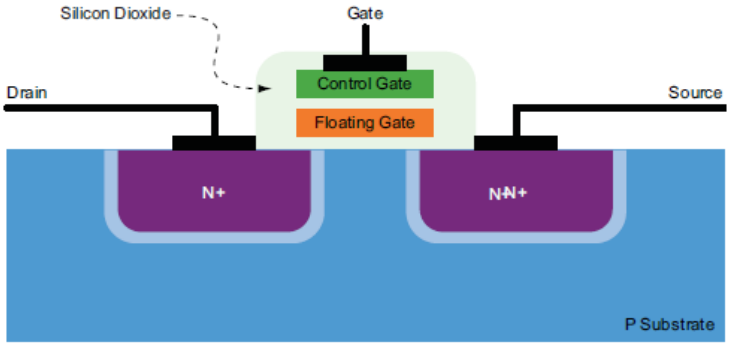

Figura 28 Estrutura de uma célula de memória FLASH (MICROSEMI, 2011b).

Analisadas as figuras 29 e 30, que representam o diagrama de blocos e a arquitetura (*floorplanning*) do SmartFusion respectivamente, torna-se possível distinguir claramente os três grandes blocos funcionais que compõe esse FPGA, quais sejam: o bloco do processador e seus periféricos (em azul na Figura 29 e em amarelo na Figura 30), o bloco do FPGA (em roxo na Figura 29 e em azul na Figura 30) e o bloco analógico (em amarelo na Figura 29 e em verde na Figura 30). Os valores de tensão nominal do SmartFusion, por sua vez, são de 3,3 V nos pinos de entrada e saída e 1,5 V no núcleo do dispositivo (*core*).

Em seguida, descreve-se detalhadamente cada um dos blocos funcionais do FPGA, o que se faz com fundamento no conteúdo dos seus manuais (*datasheets*) uma vez que não foram encontrados na literatura outros trabalhos em que o SmartFusion tenha sido adotado como objeto de estudo ou plataforma de testes.

O subsistema microcontrolador do SoC (*Microcontroller Subsystem* – MSS) é composto por um processador ARM Cortex-M3 e periféricos integrados que são interconectados através de um barramento de múltiplas camadas do tipo AHB (*Advanced High-performance Bus*) organizado no formato de uma matriz. Essa matriz permite que o processador, o FPGA em modo mestre, o controlador Ethernet e o módulo de acesso direto à memória (*Direct Memory Access* – DMA) possam atuar como mestres do barramento com a finalidade de controlar os outros módulos disponíveis no dispositivo como o FPGA, a memória embarcada não-volátil (*embedded Nonvolatile Memory* - eNVM), a memória RAM

embarcada síncrona (*embedded Synchronous RAM* – eSRAM), o controlador externo de memória (*External Memory Controller* – EMC) e os blocos analógicos (*Analog Compute Engine* – ACE). Referida organização está ilustrada na Figura 31.

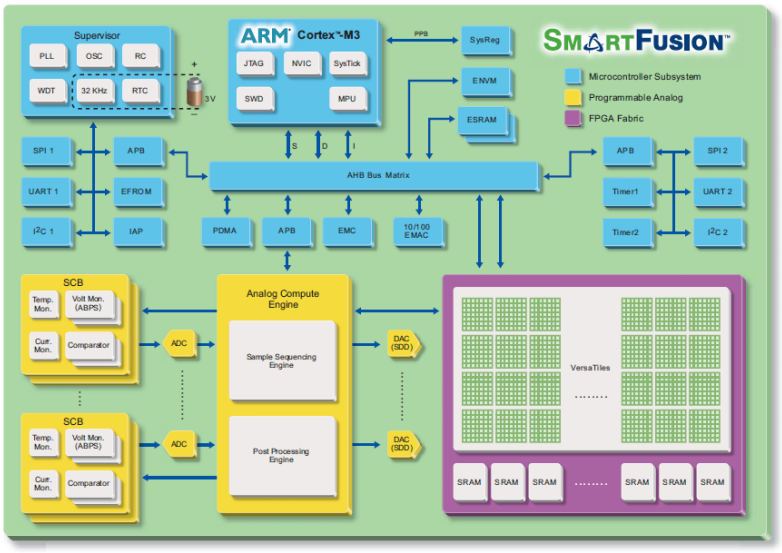

Figura 29 Diagrama de blocos do SmartFusion (MICROSEMI, 2011a).

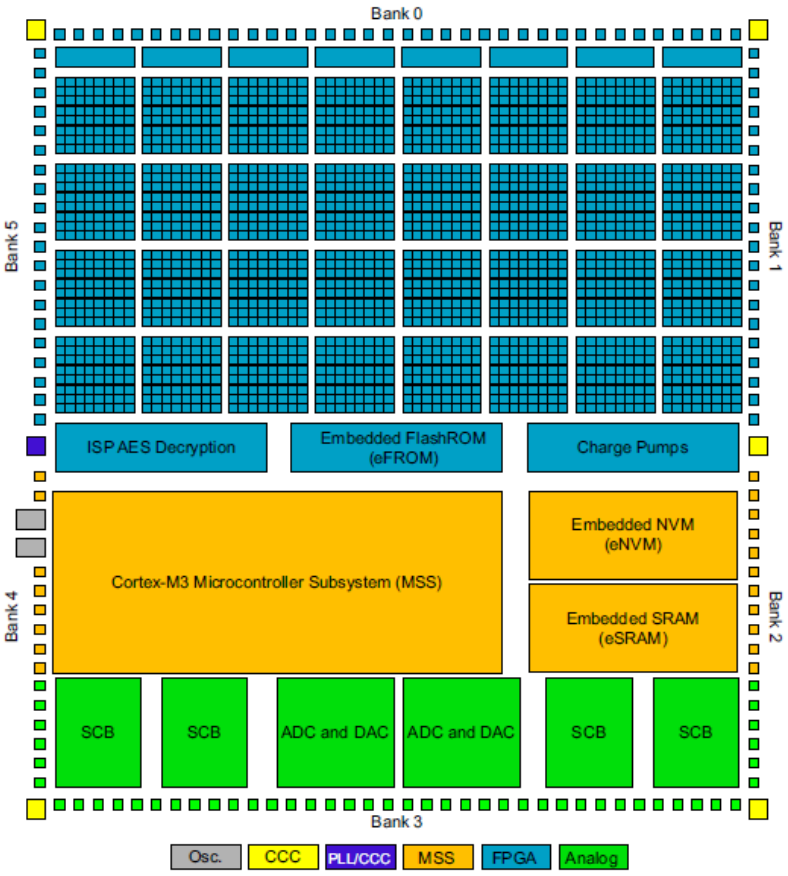

Figura 30 *Floorplanning* do SmartFusion (MICROSEMI, 2011a).

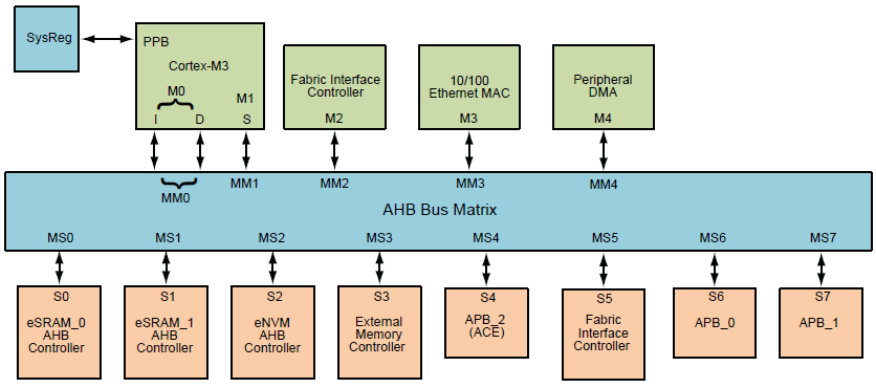

Figura 31 Organização do barramento AHB. Os blocos em verdes são os que atuam como mestres do barramento, enquanto os beges são os que atuam como escravos do barramento (MICROSEMI, 2011c).

O MSS ainda contem outros periféricos integrados como a interface SPI, a interface I²C, a interface UART, a memória ROM do tipo FLASH embarcada, o controlador Ethernet, os temporizadores, os geradores de sinais de relógio (*Phase-Locked Loop* – PLL), os osciladores, os contadores de tempo real e os periféricos já citados no parágrafo anterior (MICROSEMI, 2011a).

O processador ARM Cortex-M3 opera com instruções de 32 bits, frequência máxima de 100 MHz e três estágios de *pipeline*. Além disso, contém uma unidade de proteção de memória (*Memory Protection Unit* – MPU). Os PLLs, que são as fontes de sinais de relógio do FPGA, possuem um oscilador principal capaz de gerar uma frequência que varia de 32 KHz até 20 MHz.

No que diz respeito ao bloco referente ao FPGA propriamente dito, tem-se que é composto por uma matriz programável baseada na arquitetura ProASIC3, também da empresa Microsemi. Conforme mencionado, o FPGA é baseado em memória FLASH - não volátil - que permite que o carregamento da sua configuração não ocorra a partir de uma memória externa no momento em que é ligado, situação que ocorre em FPGAs baseados em memórias SRAM. Esta característica torna o FPGA menos vulnerável a erros na sua memória de configuração (*bitstream*). Segundo Microsemi (2011a), outro fato que torna este FPGA seguro é a localização da células de memória FLASH, situadas abaixo de sete camadas de metal, em conjunto com diversas técnicas de projeto e leiaute que são empregadas a fim de torná-lo tolerante a ataques invasivos.

A unidade básica do FPGA embarcado no SmartFusion é formada por uma arquitetura chamada *VersaTile*. Composto por quatro entradas e uma saída, o *VersaTile* pode ser configurado para implementar funções diversas, tais como: qualquer função combinacional de

três entradas, um *latch* com um sinal de limpar (*clear*) ou atribuir (*set*), um *flip-flop* do tipo D com um sinal de limpar ou atribuir e um *flip-flop* do tipo D com um sinal de habilitação e um sinal de limpar ou atribuir (MICROSEMI, 2010). A Figura 32 ilustra a arquitetura de um *VersaTile*.

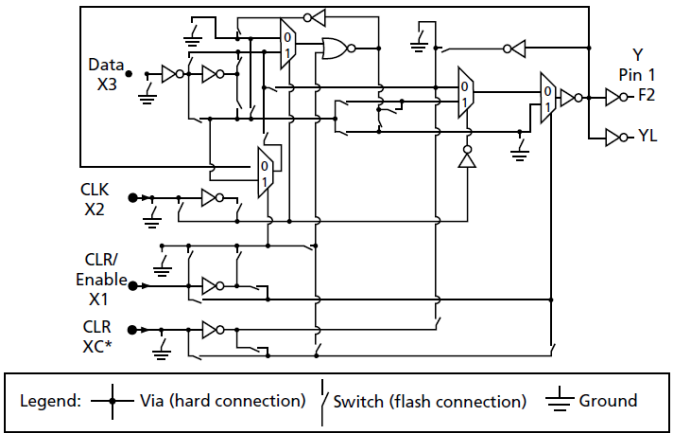

Figura 32 Arquitetura de um *VersaTile* (MICROSEMI, 2010).

O roteamento do FPGA, por sua vez, é dividido em quatro níveis de recursos: linhas locais ultra rápidas, linhas longas eficientes, linhas muito longas de alta velocidade e em uma rede global chamada de *VersaNet* (MICROSEMI, 2010). As linhas locais ultra rápidas têm a função de conectar a saída de um *VersaTile* diretamente à qualquer entrada de um dos outros oito *VersaTile* que o cercam. As linhas longas eficientes possibilitam o roteamento de longas distâncias e conexões com um grande número de entradas (*fanout*). As linhas muito longas de alta velocidade estão distribuídas em todo o FPGA e fornecem, além de um atraso mínimo, a possibilidade de haver roteamentos muito longos (doze *VersaTiles* na vertical e dezesseis na horizontal). A rede *VersaNet* é composta por sinais que possuem um atraso mínimo, um alto *fanout* e são acessíveis por pinos externos ou pela lógica interna. *VersaNets* são geralmente utilizados para distribuir sinais de relógio e sinais de *reset*.

Os blocos analógicos são divididos em duas partes: uma que é chamada de *front-end* analógico (*Analog Front-End* – AFE) enquanto que a outra é denominada de motor de computação analógica (*Analog Compute Engine* – ACE). Essa arquitetura está ilustrada na Figura 33. Tal como ocorre no caso do FPGA, que é baseado em outra família de dispositivos, a parte analógica é baseada na família de dispositivos chamada de Fusion (MICROSEMI, 2011a).

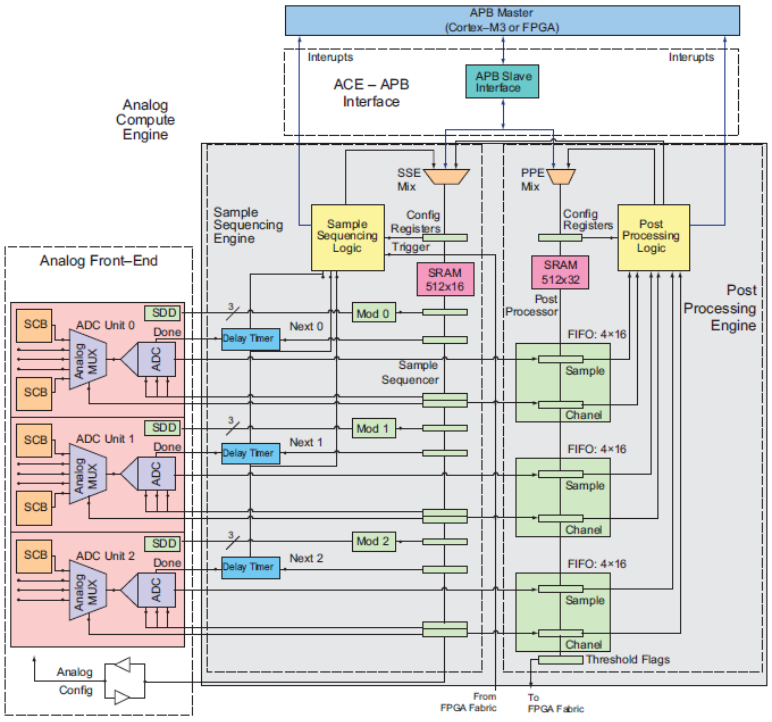

Figura 33 Arquitetura da parte analógica do SmartFusion (MICROSEMI, 2011d).

O *front-end* analógico do modelo A2F200-FG484 possui como componentes principais dois conversores analógico-digital do tipo aproximação sucessiva de 8/10/12 bits, até 600 KHz de taxa de aquisição por conversor e tensão de referência interna 2,56 V (uma tensão de referência externa de até 3,3 V pode ser aplicada) e dois conversores digital-analógico de primeira ordem do tipo sigma-delta de 8/16/24 bits, até 600 KHz de taxa de amostragem e faixa de saída de 0 até 2,56 V (MICROSEMI, 2011d).

Além dos componentes mencionados, o AFE pode executar simultaneamente múltiplos sinais analógicos através dos seus blocos de condicionamento de sinais (*Signal Conditioning Block* – SCB), que são em número de quatro no A2F200-FG484. Os SCBs são constituídos de uma combinação de pré-escalares bipolares ativos (*Active Bipolar Prescaler* – ABPS), comparadores, monitores de corrente e monitores de temperatura (MICROSEMI, 2011d).

Os módulos ABPS permitem que uma tensão maior do que a de referência possa ser aplicada nos conversores analógico-digital. Para isso, os monitores de corrente adquirem a tensão através de uma resistência de detecção externa e a convertem em uma tensão apropriada para a faixa de operação do conversor. De forma semelhante, os monitores de temperatura operam através da leitura da corrente em uma junção PN externa (um diodo ou um transistor) e a convertem internamente através de um conversor analógico-digital em uma

grandeza de temperatura (Celsius ou Kelvin). Os SCBs também incluem comparadores para monitorar sinais sem a utilização dos conversores, ou seja, as suas saídas podem ser direcionadas ao ACE.

Com relação aos monitores de corrente, tem-se, segundo Microsemi (2011d), que a saída de um monitor é ligada ao multiplexador analógico de um conversor analógico-digital para que possa ser selecionado para conversão. A sua principal função é medir variações na tensão através de uma pequena resistência externa colocada no caminho de uma corrente. O seu funcionamento ocorre através da amplificação de uma pequena tensão diferencial entre dois pinos de entrada, enquanto a tensão de modo comum é rejeitada. Com isso, a pequena tensão diferencial proporcional à corrente é desenvolvida através da resistência de acordo com a Lei de Ohm (*Tensão* = *Corrente* X *Resistência*). Ainda segundo Microsemi (2011d), o monitor de corrente tem um ganho de corrente diferencial nominal de 50 V/V, o que faz com que uma entrada de 0 a 51,2 mV seja dimensionada para a entrada do conversor analógico-digital do SmartFusion, o qual possui uma faixa de operação de 0 a 2,56 V.

O *front-end* analógico do SmartFusion é controlado e conectado ao resto do sistema via um processador dedicado, o ACE. A função do ACE é realizar o controle e a aquisição de dados dos blocos analógicos, oferecendo uma aquisição de dados mais rápida e um consumo de energia melhor quando comparado a um sistema onde o processador principal é o encarregado de monitorar os recursos analógicos. O ACE é constituído para tratar da aquisição, do sequenciamento de instruções e do pós-processamento dos conversores analógico-digital, digital-analógico e dos SCBs (MICROSEMI, 2011d).

Para este trabalho, foram utilizados diversos *kits* de avaliação do SmartFusion (*SmartFusion Evaluation Kit* – A2F-EVAL-KIT) que contêm um chip modelo A2F200-FG484 como componente principal (MICROSEMI, 2011e). Um dos principais periféricos disponíveis neste modelo de placa é a interface de comunicação USB-UART, responsável pela comunicação serial do dispositivo com um computador. Por se tratar de um *kit* de avaliação, muitas funcionalidades do chip não estão disponíveis na placa, pode-se citar, exemplificativamente, a falta de pinos dedicados para as interfaces I²C, SPI e UART. Outra desvantagem do *kit* de avaliação do SmartFusion consiste no pouco número de pinos de uso geral disponíveis na placa (quatorze), o que limita muito a comunicação do dispositivo sob teste.

O desenvolvimento de projetos para o SmartFusion é feito através de uma suíte de softwares integrada e o desenvolvimento de programas para o processador embarcado é realizado através do software *SoftConsole v3.3*, que aceita as linguagens C e C++. A

descrição de hardwares para o FPGA (que pode ser feito em VHDL ou Verilog) e o fluxo de projeto completo para o SoC (síntese, tradução, mapeamento, roteamento e geração do arquivo de programação) é feito através do programa *Libero SoC v10.1*. Por fim, a programação do FPGA é realizada através do programa *FlashPRO v10.1*.

4.3 O FPGA SPARTAN-6, MODELO XC6SLX45

Os FPGAs da família Spartan-6 são dispositivos baseado em memórias SRAM (voláteis) concebidos a partir de um processo de fabricação que tem como principais características a utilização de um nó tecnológico de 45 nm e o baixo consumo de potência a partir da utilização de cobre no seu processo de fabricação. Sua tensão de alimentação nominal é da ordem de 1,2 V e, enquanto memória volátil, exige que o dispositivo seja reprogramado a cada vez em que é ligado. Na sequência, passa-se a analisar as características relevantes para este trabalho do chip XC6SLX45.

A unidade básica do FPGA Spartan-6 e de muitos outros FPGAs da empresa Xilinx consiste na chamada *Look-up Table* (LUT). No Spartan-6, uma LUT possui seis entradas e duas saídas, todas independentes, e ainda dois registradores, conforme ilustra a Figura 34. Desse modo, é possível implementar em uma LUT qualquer função booleana com seis entradas ou duas funções booleanas com cinco entradas – desde que as duas funções tenham entradas compartilhadas – todas definidas arbitrariamente pelos geradores de função no Spartan-6 (XILINX, 2010). O atraso na propagação de um sinal em uma LUT é independente da função implementada e do número de entradas e/ou saídas utilizadas, segundo Xilinx (2010).

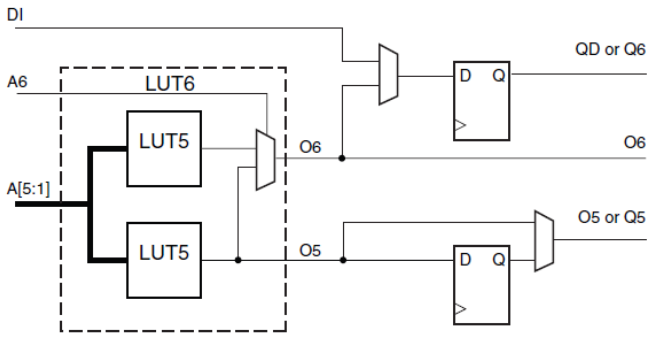

Figura 34 Estrutura de uma LUT com seis entradas (XILINX, 2010).

O FPGA Spartan-6 está organizado em blocos lógicos configuráveis, do inglês *Configurable Logic Block* (CLB), que possuem duas partes (*slices*) arranjadas sob a forma de

duas colunas verticais. Cada *slice* contém quatro LUTs, oito *flip-flops* e uma lógica digital mista (XILINX, 2010). No que diz respeito ao chip XC6SLX45, tem-se que possui 6.822 *slices*.

Com relação aos blocos de memória RAM, observa-se que o chip XC6SLX45 dispõe de 116 blocos com memória individualizada de 18 kbits, as quais podem ser endereçadas através de uma ou de duas portas, sendo síncronas e totalmente independentes as operações de leitura e escrita, compartilhando apenas os dados armazenados (XILINX, 2011a).

O Spartan-6 também dispõe de cinquenta e oito blocos dedicados de processamento digital de sinais, tradução livre de *Digital Signal Processing* – DSP, do modelo DSP48A1. Cada bloco, por sua vez, contém um somador de 18 bits seguido por um multiplicador de 18x18 bits e um somador/subtrator/acumulador de 48 bits com sinal estendido (XILINX, 2009), estruturas amplamente utilizadas no processamento digital de sinais. A Figura 35 ilustra a arquitetura do DSP48A1.

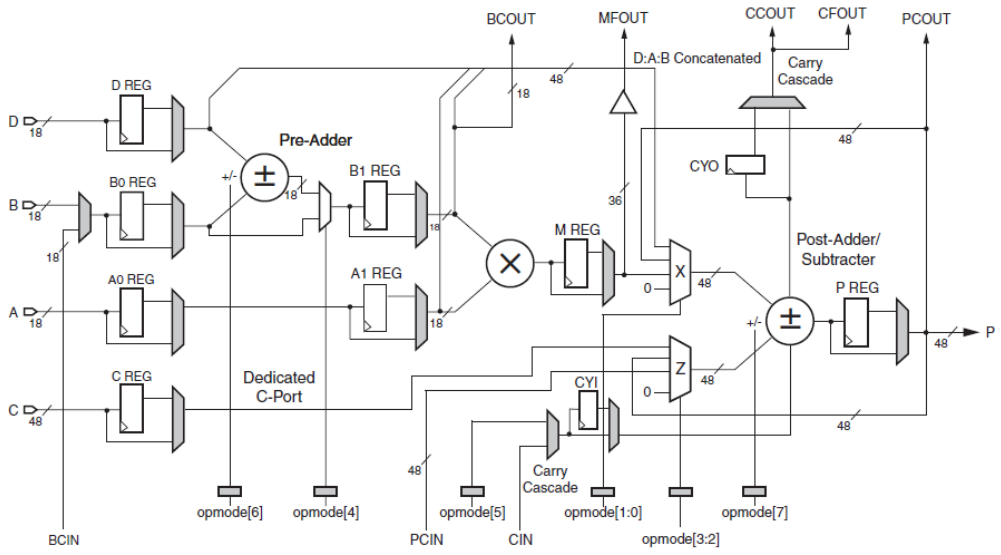

Figura 35 Arquitetura do bloco de processamento digital de sinais dedicado DSP48A1 (XILINX, 2009).

No segundo estudo de caso, utilizou-se uma placa de desenvolvimento modelo Atlys, da empresa Digilent, cujo FPGA Spartan-6 embarcado é o XC6SLX45. Dentre as características desta placa, destaca-se o módulo USB-UART, essencial à comunicação de dados entre o FPGA e um computador.

5 CARACTERIZAÇÃO DE CIRCUITOS PROGRAMÁVEIS SOB RADIAÇÃO

Os SoCs baseados em FPGAs são dispositivos complexos que necessitam de extensivos testes de radiação a fim de assegurar a sua aplicabilidade em áreas que exigem um alto grau de confiabilidade, tais como a aviônica, a militar e a aeroespacial. Em razão disso, elaborou-se uma estratégia para caracterizar simultaneamente cada um dos diferentes blocos que compõe o FPGA comercial (COTS) SmartFusion, considerando-o em sua completude e submetendo-o à radiação ionizante (TID) e aos eventos transitórios (SEEs). Esperou-se, desse modo, obter um número elevado de informações a um custo de caracterização reduzido em termos de tempo e complexidade de projeto.

Com o principal objetivo de detectar erros, não os mascarando, foi desenvolvida e embarcada uma aplicação no FPGA testado para, em um primeiro momento, executar três operações básicas, quais sejam: realizar a leitura das entradas (os componentes utilizados pela aplicação são estimulados a partir de sinais externos ao FPGA e fornecidos por equipamentos que não estão sujeitos aos efeitos da radiação como geradores de sinais ou outros FPGAs), executar a aplicação e, após o processamento, salvar e disponibilizar os resultados nas saídas dos blocos funcionais para que sejam lidos e salvos externamente ao FPGA, o que se dá, geralmente, em um analisador lógico, um osciloscópio ou um computador.

A aplicação foi gradualmente expandida para abranger um número cada vez mais significativo de componentes do FPGA. Adicionalmente às operações supracitadas e com a finalidade de realizar a detecção de erros, fez-se necessária a inserção de uma técnica de tolerância a falhas durante a aplicação dos testes. A escolha da técnica adotada e os detalhes pertinentes a sua aplicação foram abordados no capítulo anterior, Seção 3.4.

Finalizado o desenvolvimento da aplicação a ser embarcada no FPGA, realizou-se o mapeamento das entradas e saídas nas placas utilizadas em cada teste. Simultaneamente, realizou-se a montagem da configuração (*setup*) de cada experimento e o teste do *setup*. Além disso, outra plataforma, aqui denominada de placa mãe (*motherboard*), foi programada de modo a conceder suporte ao dispositivo sob caracterização através de funcionalidades, tais como: diversas frequências de relógio, sinais de *reset*, os sinais analógicos utilizados nos conversores analógico-digital e a aquisição de dados via comunicação serial. As conexões entre o dispositivo caracterizado e os equipamentos ou com a *motherboard* foram realizadas ponto a ponto.

Os dados de entrada e saída da aplicação foram observados em duas etapas diversas. Primeiramente, os dados relacionados aos efeitos de degradação causados pela dose total

ionizante (TID) foram observados através da aquisição contínua dos dados. Nesse caso, a configuração (*setup*) do experimento é inicializada antes que a fonte de radiação seja ligada para que sejam obtidos dados anteriores à irradiação. Após a inicialização da fonte de radiação, a aquisição dos dados é realizada até o momento em que o componente permanecer funcional ou até que atinja a dose esperada. Quanto aos dados de desempenho dos testes de TID e os dados dos testes de eventos transitórios (SEEs), tem-se que foram observados através de comparação. Nesse caso, os dados de entrada e de saída da aplicação foram salvos em um computador para posterior análise.

Para automatizar e conferir maior segurança à etapa de análise dos resultados, foram desenvolvidos programas para a mineração e o processamento dos dados pós-experimento, os quais foram programados na linguagem de programação C.

Assim, os seguintes resultados dos experimentos de TID foram apresentados em função da dose absorvida: consumo de corrente, tensão, temperatura e variação no atraso de propagação. Os principais dados resultantes dos experimentos de SEEs, por sua vez, foram apresentados em função da seção de choque (*cross-section*).

No que diz respeito aos estudos de caso realizados para subsidiar esta dissertação, faz-se imperioso notar que o Capítulo 4 apresentou uma visão genérica acerca da estrutura de um SoC, além dos dispositivos físicos utilizados como objeto de experimentação. A Subseção 5.1 versa acerca da caracterização do FPGA de sinais mistos SmartFusion, da empresa Actel (agora Microsemi), sob radiação (TID e SEE) através do uso de um esquema baseado em redundância diversificada dupla para detecção de erros. A Subseção 5.2, por sua vez, descreve a caracterização de um esquema baseado em um TMR diversificado e embarcado em um FPGA Spartan-6, da empresa Xilinx, sob nêutrons (SEE), com o objetivo de validar a técnica em um experimento prático uma vez que todas as abordagens encontradas na literatura e que envolvem o conceito de redundância diversifica e injeção de falhas adotaram apenas simulações em seus experimentos.

5.1 ESTUDO DE CASO I: CARACTERIZAÇÃO DO SOC SMARTFUSION

5.1.1 Caracterização dos Efeitos de Dose Total Ionizante

A rotina de testes envolvendo a dose total ionizante foi planejada para caracterizar simultaneamente o comportamento dos componentes embarcados no FPGA SmartFusion (FPGA, processador e blocos analógicos) através da técnica de detecção de erros baseada em

redundância diversificada. A Figura 36 ilustra a configuração global dos testes de dose total realizados.

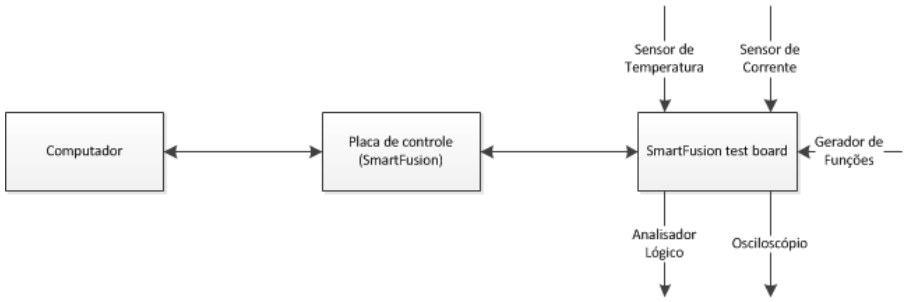

Figura 36 Visão global dos testes de dose total realizados. Um visão mais detalhada será apresentada na seção 6.2.4.

5.1.1.1 Testes Analógicos

A Figura 37 ilustra uma possível configuração para a caracterização de um conversor analógico-digital genérico no qual um estímulo conhecido é fornecido por um gerador de sinais e aplicado ao conversor analógico-digital testado. A resposta do conversor é, então, capturada por algum outro equipamento para que sejam analisados os dados de saída posteriormente (LECHNER, RICHARDSON, 2004).

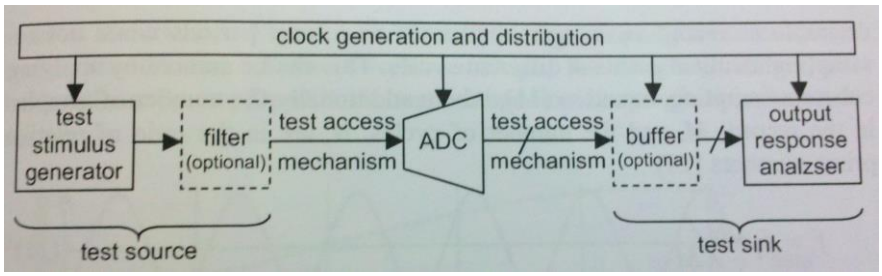

Figura 37 Configuração típica do teste de um conversor analógico-digital (LECHNER, RICHARDSON, 2004).

Em razão da arquitetura interna do SmartFusion, fez-se necessário utilizar o processador ou o FPGA em conjunto com o ACE para realizar a manipulação de dados interna ao dispositivo via barramento periférico do tipo APB (*Advanced Peripheral Bus*), aumentando a complexidade do caminho de dados. No primeiro experimento, tem-se que a aquisição de dados analógica restou completamente controlada pelo processador, enquanto que, no segundo, a coleta de dados foi completamente duplicada através do uso do processador e do FPGA.

Ainda no primeiro experimento, analisou-se um conversor analógico-digital, um sensor de corrente e um sensor de temperatura. Para o conversor, utilizou-se um gerador de sinais que fornece uma onda senoidal de 10 Hz com amplitude de zero a 2,56 V. A temperatura restou monitorada através do sensor então embarcado no chip e de um termistor monitorado fixado externamente ao SmartFusion. E a corrente, por sua vez, restou monitorada por um sensor interno ao dispositivo. A Figura 38 ilustra este esquema.

A sequência das operações foi organizada da seguinte forma: (1) espera de 3 ms, (2) amostragem do conversor analógico-digital, (3) espera de 3 ms, (4) amostragem da temperatura, (5) espera de 3 ms e (6) amostragem da corrente.

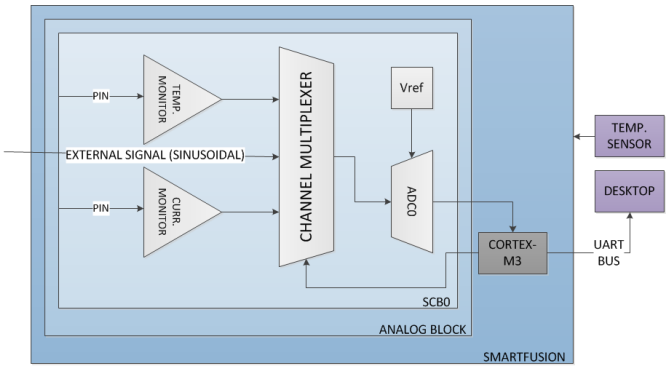

Figura 38 Organização dos blocos analógicos no primeiro teste de dose total.

Através de um esquema baseado no conceito de redundância diversificada, o segundo experimento teve por objetivo analisar não apenas os conversores analógico-digital, mas também os conversores digital-analógico. Desse modo, os conversores analógico-digital foram alimentados com uma onda senoidal com 10 Hz de frequência e amplitude de zero a 2,56 V e os conversores digital-analógico foram alimentados com as saídas digitalizadas dos conversores, sendo monitoradas as entradas e as saídas dos quatro conversores. Este esquema é ilustrado na Figura 39.

De modo semelhante ao primeiro experimento, tem-se que a sequência de operações restou organizada da seguinte forma: (1) espera de 3 ms, (2) amostragem do conversor analógico-digital 0 e do conversor digital-analógico 0, (3) espera de 3 ms, (4) amostragem do conversor analógico-digital 1 e do conversor digital-analógico 1.

À medida que o processador opera através de interrupções, tem-se que a amostragem do monitoramento de sinais possui um comportamento periódico, enquanto que um hardware embarcado em um FPGA apresenta um comportamento contínuo. Por esse motivo, as

interrupções do processador foram utilizadas como um gatilho (*trigger*) para a amostragem de dados do FPGA com a finalidade de sincronizar as duas aquisições de dados.

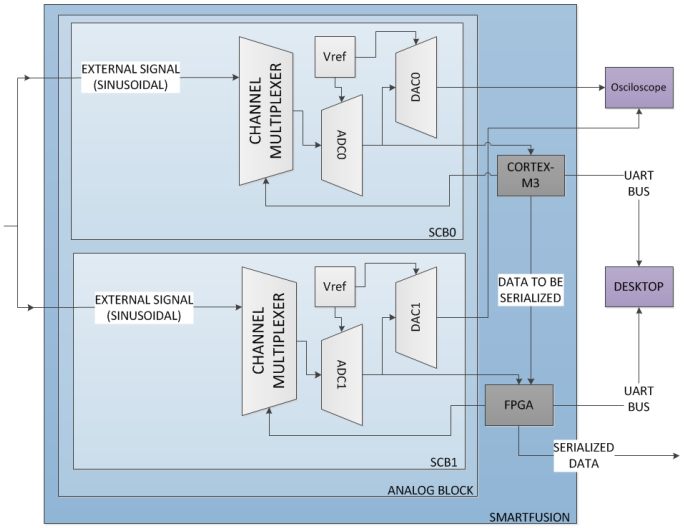

Figura 39 Organização dos blocos analógicos no segundo teste de dose total.

5.1.1.2 Testes Digitais

Os circuitos de teste embarcados no FPGA têm o objetivo de coletar uma maior quantidade de detalhes acerca da confiabilidade do dispositivo quando submetido ao contexto de dose total ionizante. Em outros termos, tem-se que o uso dos circuitos desenvolvidos objetivou investigar a influência da frequência de operação no atraso de propagação de sinais em decorrência do aumento na degradação provocada pela radiação ao longo do tempo.

Para o primeiro experimento, foram desenvolvidos dois circuitos diferentes, quais sejam: um contador síncrono de quatro bits (duas instâncias, uma com frequência de relógio de 40 MHz e a outra de 20 MHz) e um oscilador em anel de noventa e nove estágios. Todas as unidades básicas dos circuitos foram posicionadas manualmente lado a lado no FPGA. Cada estágio do oscilador em anel corresponde a um *VersaTile* no FPGA e as frequências de relógio foram fornecidas por outra SmartFusion, que não estava sob os efeitos da radiação ionizante. A Figura 40 ilustra esses circuitos.

No que diz respeito ao oscilador em anel, tem-se que a degradação foi investigada através do monitoramento da frequência durante o transcorrer do tempo de experimento. Para os contadores, a degradação foi analisada por meio da relação entre a frequência de relógio de entrada e o resultado final (valor “15”) na saída de cada contador.

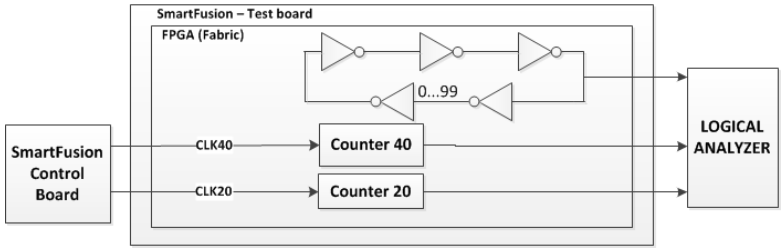

Figura 40 Configuração dos circuitos auxiliares implementados no FPGA no primeiro experimento de dose total.

O segundo experimento ocorreu de forma assemelhada ao primeiro no que se refere aos circuitos auxiliares embarcados no FPGA, à exceção das seguintes especificações: ambos os contadores eram assíncronos, haviam dois osciladores em anel (um com noventa e nove estágios e o outro com quarenta e nove estágios) e um circuito de serialização implementado no esquema baseado em redundância diversificada. A degradação dos contadores assíncronos foi analisada em função do intervalo de tempo entre dois resultados finais sequenciais (valor "15").

Nesse sentido, faz-se relevante rememorar que uma das desvantagens no uso de uma placa de avaliação do SmartFusion (*evaluation kit*) em detrimento de uma placa de desenvolvimento do SmartFusion (*development kit*) consiste no baixo número de pinos de entrada e de saída, característica que restringe significativamente o número de componentes a serem testados.

5.1.1.3 Testes Relacionados ao Processador e ao Esquema Redundante e Diversificado de Sinais Mistos

Durante o primeiro experimento, o comportamento do processador Cortex-M3 à radiação ionizante, aqui assumido como o componente mais robusto do SmartFusion, foi observado através da eficácia da coleta de dados durante a realização do primeiro experimento. Para o segundo experimento, a performance do processador Cortex-M3 e do FPGA foram analisadas através de um esquema redundante e diversificado, além do monitoramento através da aquisição de dados. Esse esquema consiste na aquisição, manipulação e transferência de dados no SmartFusion através de dois caminhos totalmente independentes, sendo um controlado pelo processador Cortex-M3 e o outro pelo FPGA. A abordagem descrita revela-se importante à medida que cada cópia (e o dispositivo como um todo) é composta por componentes distintos e que operam de maneira distinta, o que tende a

resultar diferentes níveis de degradação para uma mesma dose acumulada. A Figura 41 ilustra a organização proposta.

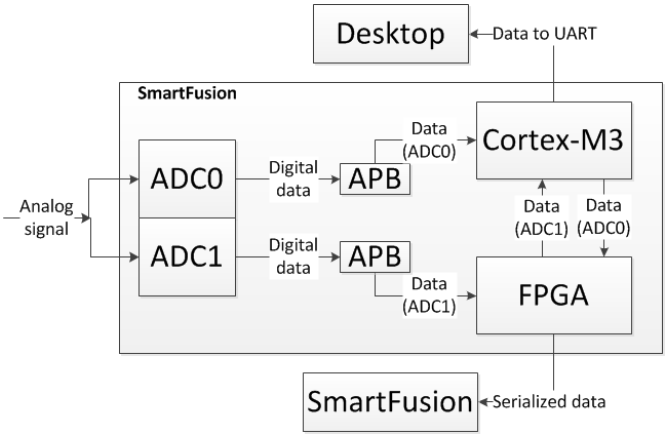

Figura 41 Esquema redundante de diversificado implementado no segundo teste de dose total.

5.1.1.4 Montagem dos Testes

Os parâmetros elétricos testados dos sinais de entrada e de saída dos SmartFusion foram observados e gravados em tempo real durante as irradiações. Os dispositivos foram irradiados através do uso de um feixe colimado de raios gama provenientes de uma fonte de Cobaldo-60 disponível no Instituto de Estudos Avançados da Aeronáutica (IEAv), localizado em São José dos Campos - SP, Brasil.

No primeiro experimento, o FPGA foi irradiado a uma taxa de 2,22 krad(Si)/h (0,616 krad(Si)/s) até uma dose total de 79,92 krad(Si) enquanto que, no segundo experimento, o mesmo modelo de FPGA foi irradiado a uma taxa de 2,25 krad(Si)/h (0,625 krad(Si)/s) até uma dose total de 78,75 krad(Si). Ambas as irradiações foram realizadas a uma temperatura ambiente de 24 ± 0,5 °C. O chip foi coberto com uma camada de acrílico de 5 mm de espessura com a finalidade de estabelecer uma condição de equilíbrio eletrônico e assim poder calcular a dose absorvida no silício a partir da dose medida no ar com uma câmara de ionização (KASTENSMIDT et al., 2011).

Foram coletadas medidas funcionais no FPGA e no ARM Cortex-M3 com o auxílio de um analisador lógico de taxa de aquisição de 2ns de precisão e um osciloscópio com largura de banda de 1 GHz. A temperatura da superfície do chip foi medida utilizando um termistor monitorado. Os equipamentos utilizados nos experimentos estão especificados na Figura 42, na qual o bloco DUT (*Device Under Test* ou Dispositivo Sob Teste em tradução livre para o

português) corresponde ao SmartFusion. A Figura 43 ilustra o experimento montado dentro da sala de irradiação.

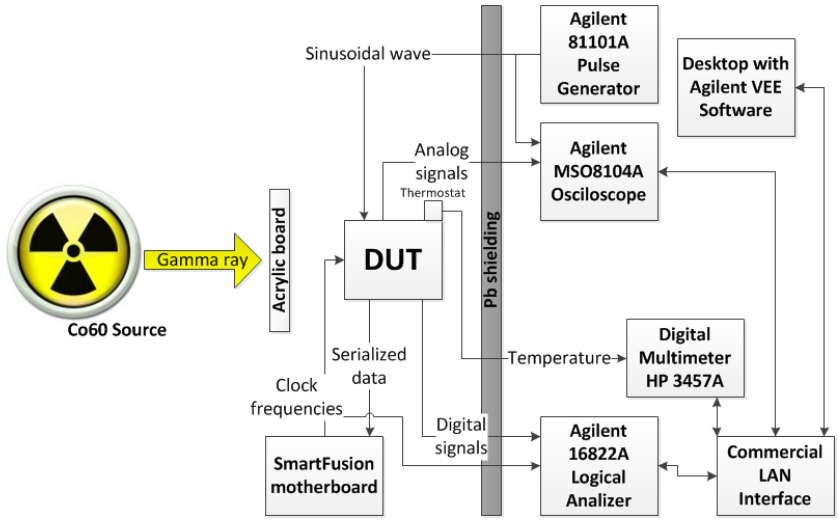

Figura 42 Esquemático da configuração dos testes de dose total ionizante.

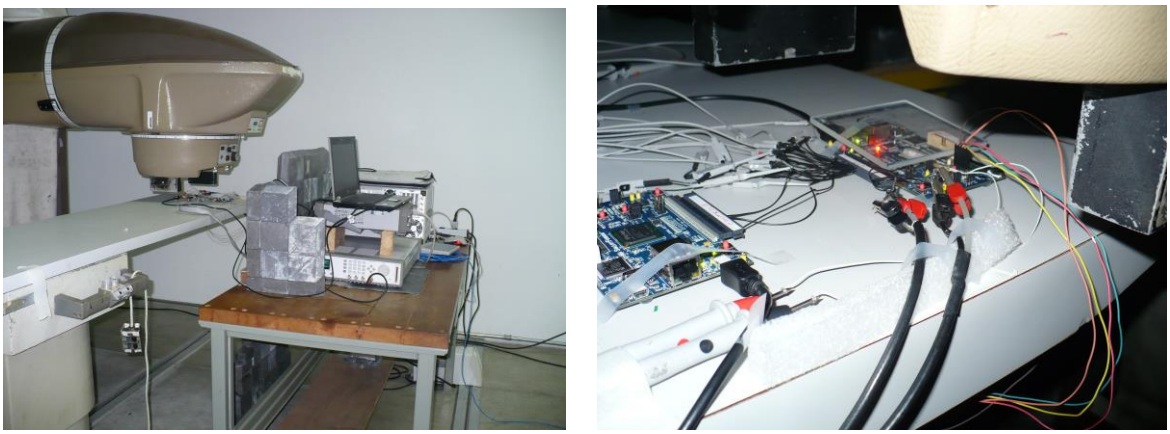

Figura 43 Fotografias da configuração dos testes dentro da sala de irradiação.

Durante as irradiações, uma aquisição de dados era realizada a cada 15 minutos (0,555 krad(Si)) no primeiro experimento e a cada 10 minutos (0,375 krad(Si)) no segundo experimento e o controle, incluindo a aquisição e o armazenamento de dados, ocorreu remotamente, sendo todos os arquivos armazenados para a análise posterior.

Em razão do pequeno número de pinos de entrada e de saída disponíveis, no teste envolvendo o processador ARM Cortex-M3, os resultados dos conversores analógico-digital foram armazenados em um computador através de uma comunicação serial do tipo UART. Já no experimento envolvendo o FPGA, implementou-se um circuito de serialização para transferir os dados analógicos convertidos à placa de controle para, só então, transferi-los a

um computador via comunicação serial do tipo UART. Importante destacar que a comunicação serial do SmartFusion com o computador ocorre através de um módulo do tipo USB-UART integrado à placa de avaliação, ou seja, o padrão UART converte-se automaticamente ao padrão USB, o que facilita a comunicação do FPGA com qualquer computador que disponha de uma entrada do tipo USB.

5.1.2 Resultados dos Testes de Dose Total Ionizante

5.1.2.1 Efeitos na Corrente e na Temperatura

O consumo de corrente no dispositivo foi medido através do uso de um sensor embarcado no FPGA durante a realização do primeiro experimento, resultado apresentado na Figura 44. Analisando o gráfico desta figura, pode-se notar a ocorrência de um pico de corrente em uma dose ionizante de aproximadamente 38 krad(Si). Após esse evento, em 42,73 krad(Si) ela atinge um consumo de quase cinco ordens de grandeza maior que o seu valor inicial.

Os valores observados após a dosagem de 42,73(Si) tornam-se constantes, o que pode ser justificado em razão das limitações do conversor analógico-digital, ou seja, os valores da corrente provavelmente atingiram valores maiores que os amostrados, ultrapassando a faixa de operação do conversor analógico-digital.

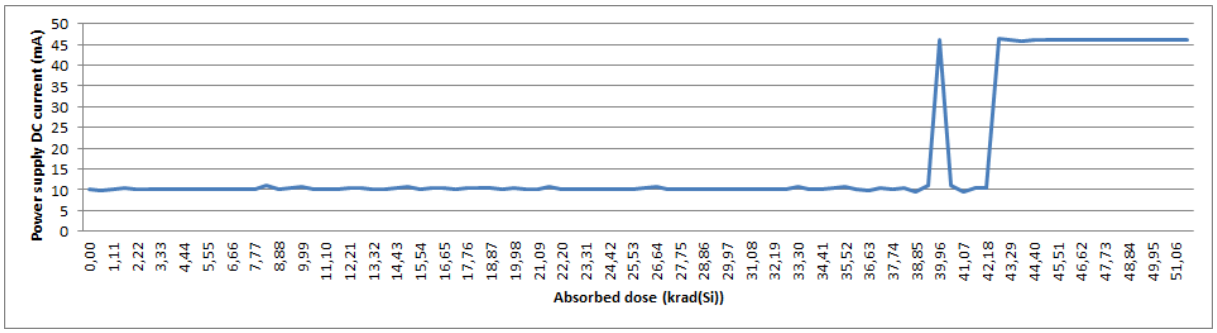

Figura 44 Consumo de corrente no SmartFusion em função da dose absorvida com o decorrer do tempo de irradiação.

Para as medições de temperatura, utilizou-se dois sensores nos experimentos, um embarcado no FPGA e outro posicionado sobre ele. Os resultados obtidos são apresentados na Figura 45.

O sensor embarcado parou de operar, no primeiro experimento, a uma dose de 16,65 krad(Si) e, no segundo experimento, a uma dose de 15,94 krad(Si). Importante notar que a

temperatura começou a aumentar logo após o consumo de corrente atingir o seu pico no primeiro experimento.

Através da comparação dos resultados obtidos entre os sensores internos e externos, faz-se pertinente concluir que o sensor embarcado no SmartFusion apresentou resultados similares antes da sua falha funcional no primeiro experimento se comparado com os resultados do sensor externo. Contudo, no segundo experimento, a diferença entre os sensores interno e externo foi significativa, atingindo até três graus Celsius de diferença.

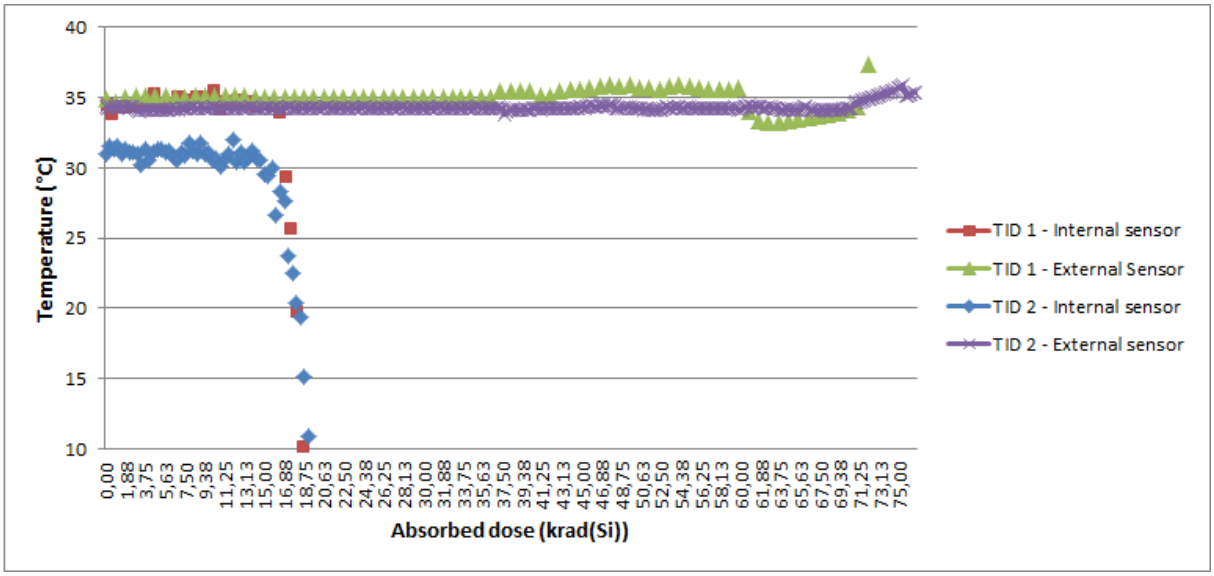

Figura 45 Variação da temperatura no SmartFusion em função da dose absorvida com o decorrer do tempo de irradiação.

Os dados de corrente e de temperatura são extremamente importantes no que diz respeito à análise dos efeitos de dose total ionizante, como o atraso na propagação de sinais e a ocorrência de falhas funcionais. Isso porque é possível observar que a corrente de fuga pode aumentar drasticamente em processos de tecnologias comerciais (não tolerantes à radiação) quando submetidos à radiação ionizante. Segundo Faccio e Cervelli (2005), em tecnologias semelhantes à do SmartFusion (130 nm), o aumento da corrente de fuga em um único transistor pode variar de alguns nA até poucos μA dependendo do fabricante e da quantidade de carga acumulada. Desse modo, tem-se que o rápido aumento da corrente (apresentado na Figura 44) já era esperado em razão do acúmulo de radiação ionizante, o que causa um aumento das correntes de fuga nos MOSFETs e nos transistores de *floating gate*.

5.1.2.2 Alterações no Atraso de Propagação

A variação do atraso em função da degradação causada pelo acúmulo de radiação ionizante seguiu, no primeiro experimento, os efeitos da corrente e da temperatura e, no segundo experimento, apenas aos efeitos da temperatura.

Com relação aos osciladores em anel implementados nos experimentos, tem-se que aqueles compostos por noventa e nove estágios estavam operando a 50 MHz enquanto que o de quarenta e nove estágios operando a 100 MHz. Os resultados referentes ao atraso na propagação dos sinais dos osciladores estão ilustrados no gráfico da Figura 46. Analisada a figura, observa-se que, em uma dose de 28 a 30 krad(Si), atingiu-se 20% de degradação dos três anéis, contudo, após esse ponto, a porcentagem de degradação de cada anel tornou-se significativamente diferente.

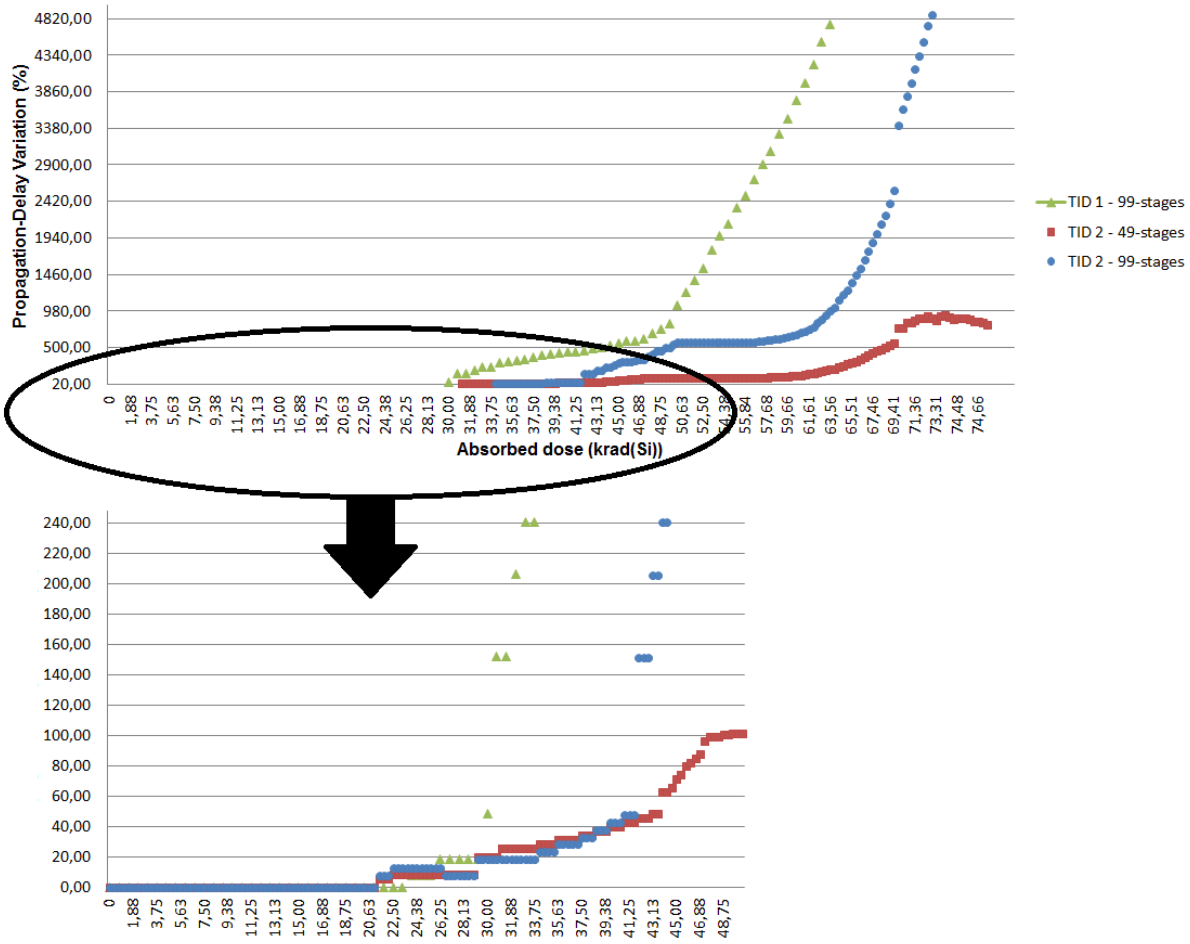

Figura 46 Variação do atraso expressa em porcentagem pela dose absorvida nos osciladores em anel embarcados no FPGA do SmartFusion.

No oscilador em anel do primeiro experimento, observa-se que a sua curva de degradação apresenta uma maior inclinação após a dose absorvida onde a corrente e a temperatura começaram a aumentar, chegando a atingir 4740% de degradação. Esse cenário pode ser observado de forma assemelhada nos osciladores em anel do segundo experimento, em que o mesmo aumento ocorre após o aumento de temperatura, chegando a atingir 4870% de degradação no oscilador maior e 916% no oscilador menor. No segundo experimento, pode-se ainda observar que o aumento no percentual de degradação do menor (e mais rápido) oscilador inicia quase 20 krad(Si) após o início da degradação no oscilador maior. Uma justificativa para esse comportamento consiste no fato de que em uma cadeia de portas lógicas (neste caso, inversores), o sinal adquirido contém o atraso intrínseco de todos os seus elementos. A medida que o dispositivo acumula radiação ionizante, o atraso intrínseco de cada porta lógica aumenta. Espera-se então que, quanto menor a cadeia, menor será o atraso acumulado em função da degradação.

No caso dos contadores, os circuitos apresentaram um comportamento distinto se comparados com os osciladores em anel, independentemente de o contador ser ou não síncrono. Isso porque, em ambos os experimentos, pode-se observar que os contadores começaram a apresentar um rápido aumento no atraso de propagação logo após a diminuição da temperatura – aproximadamente 60 krad(Si) para o primeiro experimento e 74 krad(Si) para o segundo experimento – o que pode indicar uma falha funcional no FPGA do SmartFusion. Além disso, é razoável esperar que o consumo de potência dinâmica das portas do circuito seja menor após uma determinada acumulação de dose ionizante do que o consumo de potência no estágio em que o dispositivo encontra-se completamente operacional e livre de radiação, resultando na diminuição da corrente. Os resultados obtidos estão ilustrados no gráfico da Figura 47.

A relação da temperatura e da corrente com a ocorrência de uma falha funcional no FPGA pode ser observada no primeiro experimento e também no trabalho Kastensmidt et al. (2011), no qual o FPGA ProASIC3E foi submetido a TID. Em ambos, pode-se verificar o comportamento similar da corrente e da temperatura em função dos efeitos causados pelo acúmulo de radiação ionizante, reforçando a probabilidade de ocorrência de uma falha funcional no FPGA do SmarFusion para o segundo experimento.

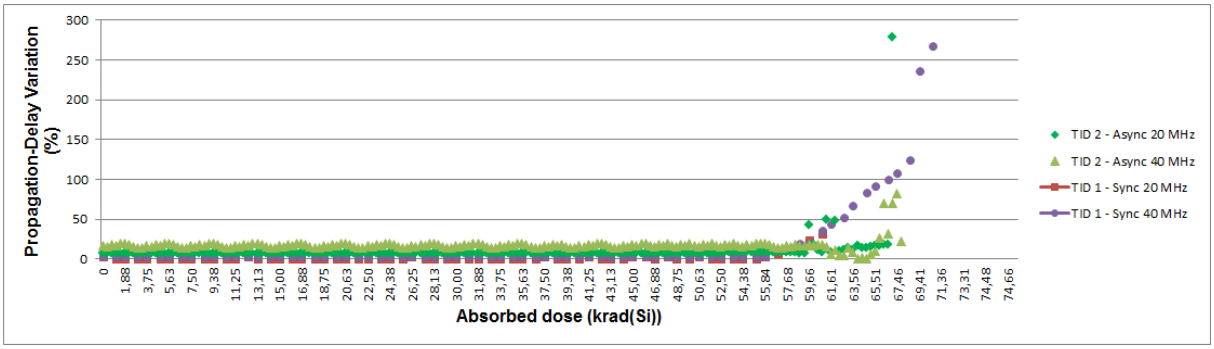

Figura 47 Variação do atraso expressa em porcentagem pela dose absorvida nos contadores síncronos e assíncronos embarcados no FPGA do SmartFusion.

5.1.2.3 Aquisição Redundante dos Dados

No primeiro experimento, em que a aquisição de dados foi realizada somente através do processador ARM Cortex-M3 em conjunto com o barramento UART, ocorreu uma falha inesperada que interrompeu a comunicação de dados a uma dose de 51,61 krad(Si). Desse modo, os dados obtidos em doses superiores correspondem aos adquiridos a partir do analisador lógico que fazia parte do *setup* do experimento.

A fim de comparar a confiabilidade do caminho de dados composto pelo processador ARM Cortex-M3 e do barramento UART com outro caminho composto apenas pelo FGPA, realizou-se uma aquisição de dados redundante e diversificada no segundo experimento. Como resultado, observou-se que o circuito de serialização de dados implementado no FPGA apresentou uma falha funcional a uma dose acumulada de 72,12 krad(Si), coincidindo com o valor máximo de temperatura registrado durante o experimento. Enquanto isso, o caminho de dados controlado pelo processador mostrou-se funcional até o final da irradiação e sem alterações significativas de desempenho.

5.1.2.4 Resultados dos Conversores de Dados

No que diz respeito aos conversores de dados, observa-se que apenas um conversor analógico-digital foi testado durante o primeiro experimento e que não restou possível a realização de uma análise dinâmica e estática dos dados em razão do número insuficiente de pontos obtidos por amostra. Todavia, através de uma análise macroscópica dos dados convertidos, notou-se a ocorrência de anomalias nos valores convertidos na mesma faixa de dose acumulada quando a corrente e a temperatura começaram a aumentar, o que ocorreu em torno de 38 krad(Si). Posteriormente, os valores convertidos tornaram-se semelhantes aos obtidos no início do experimento.

Ainda quanto ao primeiro experimento, tem-se que os dados coletados do conversor analógico-digital e dos sensores embarcados pelo processador ARM Cortex-M3 e enviados via barramento UART, pararam de ser salvos com 51,61 krad(Si) de dose acumulada devido a ocorrência de uma falha funcional em um dos componentes envolvidos na aquisição de dados. Nesse caso, é importante destacar que o processador apresentou um comportamento regular e sem perda de desempenho até o momento em que ocorreu a falha funcional na aquisição de dados.

No segundo experimento, foram testados ambos os conversores analógico-digital e digital-analógico. Os conversores analógico-digital foram estimulados conforme a descrição constante na subseção 6.2.1 deste trabalho, sendo que a principal função do processador ARM Cortex-M3 e do FPGA foi realizar a leitura dos dados convertidos por cada ADC, enviando-os a cada um dos DACs, conforme ilustrado pela Figura 41. Nesse caso, em razão da baixa frequência do sinal aplicado e do fato de que o teste foi realizado remotamente, condição que impediu maiores ajustes no *setup* do experimento, não foi possível atingir a resolução necessária para realizar uma análise precisa dos dados via Transformada Rápida de Fourier (*Fast Fourier Transform* – FFT).

Contudo, observados os dados provenientes das saídas dos conversores digital-analógico, foi possível observar a ocorrência de janelas de degradação e inatividade através de uma análise baseada no Valor Quadrático Médio, do inglês *Root Main Square* (RMS). No que diz respeito às janelas de degradação e inatividade, descritas em Franco, Zong e Agapito (2006) e recentemente discutidas em Balen et al. (2011a), tem-se que o evento consiste em um intervalo de tempo específico em que, a um certo nível de dose acumulada, o dispositivo deixa de funcionar para, posteriormente, recuperar sua funcionalidade em doses acumuladas mais elevadas do que o limite superior da janela. Os resultados dessa análise são apresentados na Figura 48. Destacando os efeitos causados pelas janelas de inatividade, a Figura 49 ilustra um exemplo de sinal adquirido em quatro diferentes doses acumuladas. Assim, uma vez que os dados convertidos pelos conversores analógico-digital não apresentaram o comportamento descrito, tem-se que não foram afetados por esse efeito.

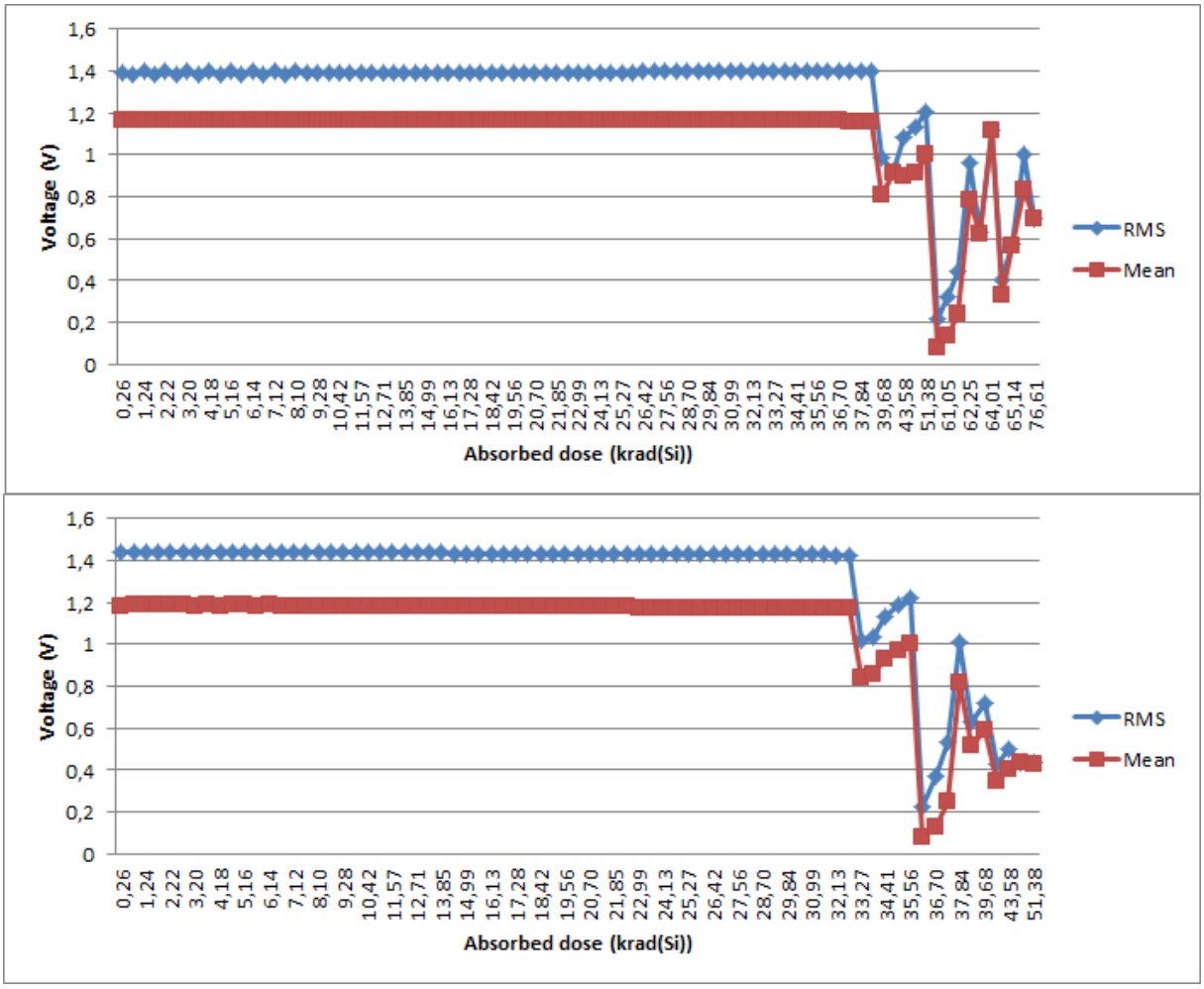

Figura 48 Valores RMS obtidos dos valores amostrados pelos conversores analógico-digital, sendo um controlado pelo processador (a) e o outro pelo FPGA (b).

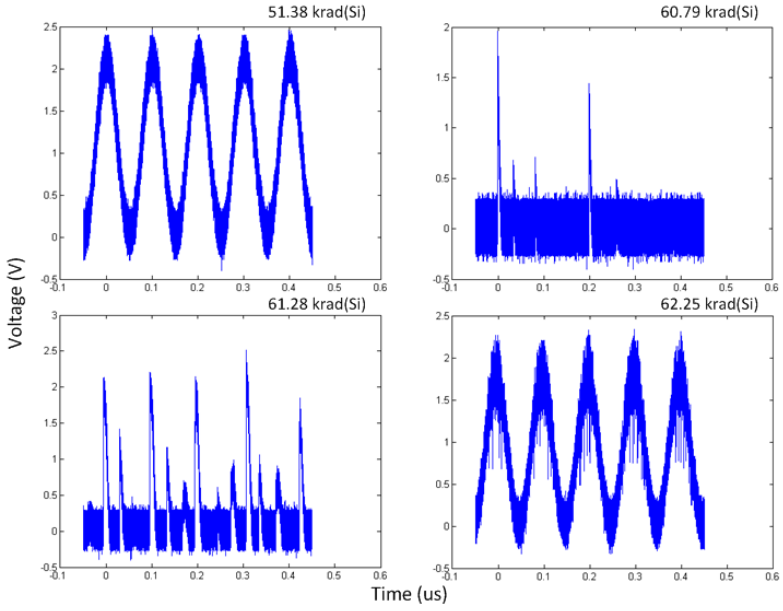

Figura 49 Exemplo da ocorrência de uma janela de inatividade parcial em um dos conversores digital-analógico.

5.1.2.5 Efeitos Causados pelo *Annealing*

No segundo experimento, observa-se que o *annealing* durou três semanas (504 horas) em temperatura ambiente ($24°C \pm 4°C$). Após esse período, a porcentagem de degradação no atraso do oscilador em anel de noventa e nove estágios diminuiu de 5970% (0,62 MHz) para 1650% (2,72 MHz), enquanto que no oscilador em anel de quarenta e nove estágios diminuiu de 805% (1,18 MHz) para 396% (4,84 MHz). O ARM Cortex-M3 e o barramento UART também se mostraram funcionais após o período de *annealing*. Apesar de funcionais, os conversores analógico-digital passaram a apresentar um erro de escala variando de 25 mV até 46 mV. Os outros circuitos não forneceram nenhum sinal de recuperação. No primeiro experimento, não foi realizado nenhum *annealing*.

Em paralelo ao segundo experimento, um segundo SmartFusion foi irradiado até a dose acumulada de 25 krad(Si) para outros fins. Dentre os dados obtidos neste outro experimento, observou-se que ao final da irradiação não foi mais possível realizar os procedimentos de verificação, apagamento e programação do SoC. Consequentemente, verifica-se que essas operações também não puderam ser realizadas após o período de *annealing* de ambos os FPGAs irradiados no segundo experimento.

5.1.3 Caracterização dos Efeitos de *Single Event Effects*

O teste de *Single Event Effects* foi realizado com a finalidade de analisar o comportamento do máximo possível de componentes embarcados no FPGA SmartFusion. Para tanto, utilizou-se uma proposta semelhante à adotada nos testes de dose total ionizante, em que a aplicação desenvolvida fez uso do processador, do FPGA e dos conversores analógico-digital em conjunto com a utilização da técnica de detecção de erros baseada em redundância diversificada.

5.1.3.1 Arquitetura de Teste Desenvolvida

Para a realização do teste de *Single Event Effects*, desenvolveu-se uma arquitetura baseada no projeto desenvolvido para o segundo experimento de dose total ionizante, no qual se utilizou um esquema de redundância modular dupla e cuja função principal é a de realizar a aquisição de dados analógicos, conforme ilustrado pela Figura 41. Ainda que as cópias redundantes desempenhem função idêntica, tem-se que foram implementadas em níveis diferenciados no SmartFusion porquanto uma cópia é implementada via software e embarcada

no processador ARM Cortex-M3 enquanto que a outra é implementada em hardware no FPGA. A função principal das cópias consiste em realizar o controle a manipulação dos dados provenientes dos conversores analógico-digital.

A cópia implementada via software foi desenvolvida utilizando-se as bibliotecas padrão da linguagem de programação C e as bibliotecas proprietárias da empresa Microsemi responsáveis pela manipulação do subsistema microcontrolador do SmartFusion. A cópia implementada via hardware no FPGA, por sua vez, tem seu código composto por uma máquina de estados (*Finite State Machine* – FSM) responsável pela leitura e a manipulação dos dados provenientes do barramento do MSS e de um circuito de serialização, ambos implementados na linguagem de descrição de hardware VHDL. A Figura 50 ilustra em detalhes a arquitetura da aplicação em que um sinal analógico idêntico é aplicado a os conversores analógico-digital do SmartFusion.

O fluxo de dados segue a seguinte ordem: primeiro, uma amostra do sinal analógico de entrada é adquirido pelos conversores analógico-digital e processados pelo ACE; segundo, os valores convertidos são alocados em endereços distintos do barramento de dados (AHB) do subsistema microcontrolador; por fim, ambos ARM Cortex-M3 e FPGA leem os seus respectivos valores do barramento os processam.

O processador e o FPGA foram configurados para operar a 10 MHz enquanto que os conversores analógico-digital foram configurados para operar a 2,5 MHz (aproximadamente 26 ksps), com uma resolução de 12 bits e um tensão de referência interna de 2,56 V. Conforme observado, uma importante diferença que afeta a amostragem dos dados consiste no fato de que a sua aquisição via FPGA se dá de forma contínua, o que não acontece no processador, cuja aquisição ocorre periodicamente. Desse modo, utilizou-se as interrupções do processador como um gatilho (*trigger*) para a amostragem de dados do FPGA para fins de sincronizar as duas aquisições de dados.

5.1.3.2 Circuitos Digitais Complementares Implementados

Como circuitos de testes, foram implementados no FPGA do SmartFusion dois registradores de deslocamento, cada um com mil estágios, para aumentar a área de abrangência sensível da matriz programável. Ambos os circuitos foram configurados de modo a ter todos os seus bits em zero e a operar a 10 MHz, mesma frequência de relógio dos circuitos implementados e do processador.

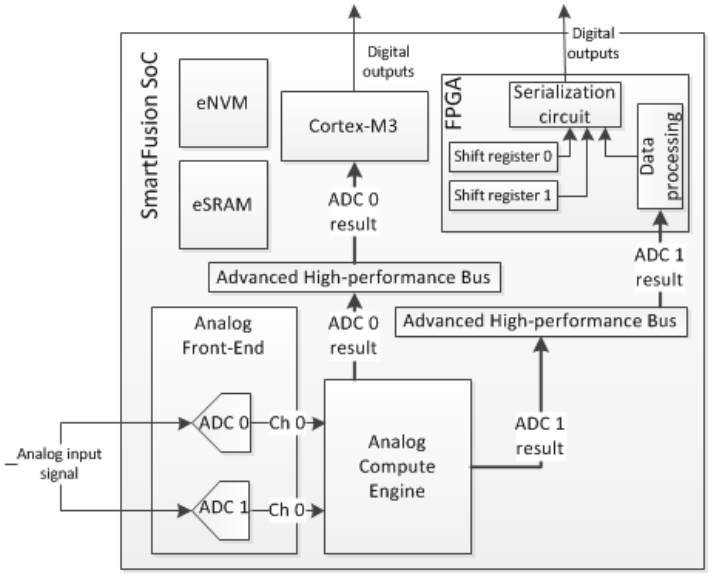

Figura 50 Arquitetura redundante e diversificada implementada no SmartFusion para o teste de SEEs.

Para possibilitar a aquisição de dados redundantes, também implementou-se um circuito de serialização no FPGA.

Todos os circuitos foram manualmente posicionados no FPGA e, além disso, garantiu-se que nenhuma parte dos circuitos implementados fosse simplificada nos processos de síntese e mapeamento dos códigos. Os circuitos mencionados estão ilustrados na Figura 50.

5.1.3.3 Montagem do Teste

O *setup* do teste de *Single Event Effects* é composto pelo dispositivo sob teste (*Device Under Test* – DUT) e uma placa de controle, estando ambos conectados ponto-a-ponto. Ambas as placas são de avaliação (A2F-EVAL-KIT) e contém um SmartFusion modelo A2F200-FG484.

Todos os dados coletados foram transferidos para um computador via interface USB-UART da placa de controle e armazenados em arquivos de texto para uma análise posterior, o que ocorreu em tempo real. Além disso, ainda que a alimentação da A2F-EVAL-KIT pudesse ter sido realizada via interface USB através de um computador, o DUT foi alimentado através de um extensor USB para evitar a ocorrência de um eventual *latch-up* no SmartFusion, o que poderia danificar o computador. A Figura 51 ilustra as conexões existentes entre a placa de controle e o DUT.

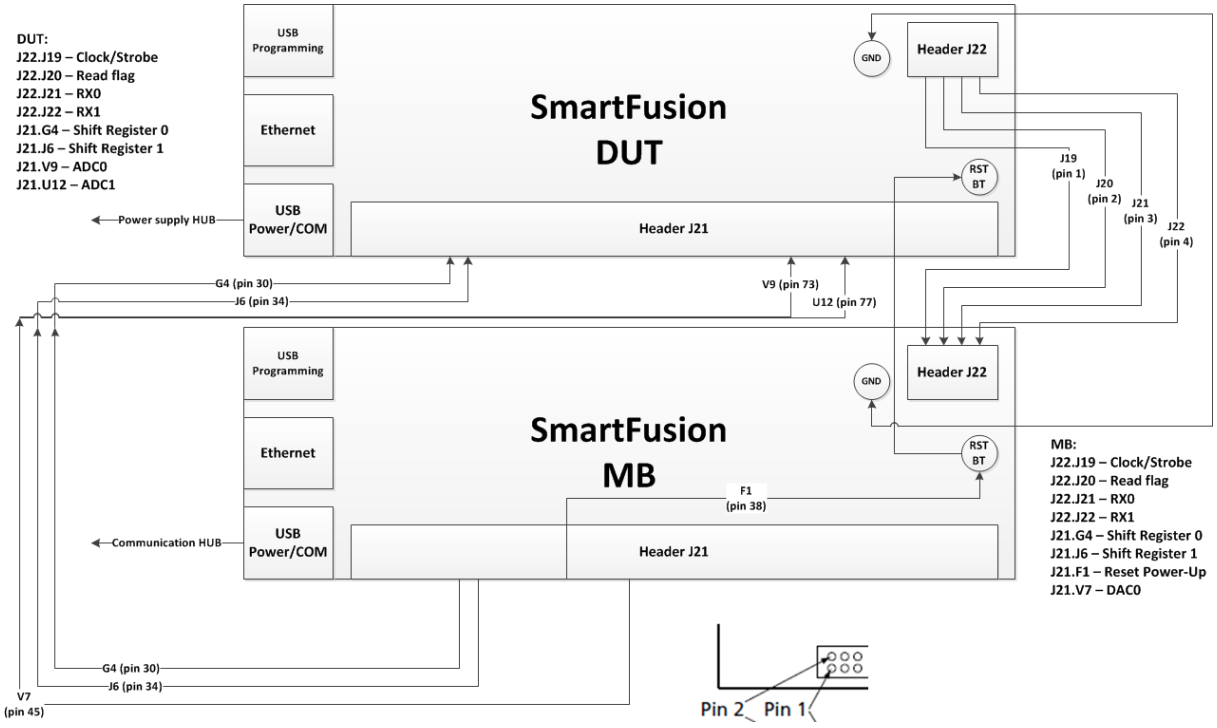

Figura 51 Ilustração das conexões entre a placa de controle (SmartFusion MB) e o DUT no experimento de SEEs.

A placa de controle possui embarcados os seguintes circuitos: um circuito do tipo *power-on reset* para assegurar que todos os outros circuitos irão iniciar em um estado conhecido após o chip ser inicializado (ou seja, ser ligado e realizar um ciclo de reprogramação); um circuito gerador sinal que, em conjunto com dos conversores digital-analógico, é responsável por gerar um sinal periódico no formato de uma rampa com uma frequência de 10 Hz, uma tensão do bit menos significativo (*Least Significant Bit Voltage* - V_{lsb}) de 5 mV e uma amplitude que varia de 0 a 2,56 V; e, ainda, um circuito receptor responsável pela aquisição dos dados provenientes do DUT. O DUT é composto pelas implementações descritas nas subseções 6.2.1 e 6.2.2.

O circuito *power-on* é composto por dois contadores de dezessete bits em cascata, sendo que o primeiro contador possui a função de gerar um atraso de 5 ms para o segundo, que, por sua vez, gera um sinal de *reset* para o resto da placa de controle e para o DUT.

O circuito receptor possui duas funções: primeiramente, recebe os valores convertidos do DUT e os envia ao módulo UART da placa de controle. Posteriormente, o circuito receptor detecta inversões de bit nos registradores de deslocamento através do seguinte esquema: se um bit "1" é recebido, então os próximos novecentos e noventa e nove bits de cada registrador de deslocamento são analisados e, a cada bit "1" detectado, um contador é incrementado. Se

uma inversão de bit é detectada nos registradores de deslocamento, o resultado do contador é enviado para um computador via barramento UART e salvo para posterior análise.

O teste de SEE foi realizado em um acelerador de partículas gerador de nêutrons localizado no *Rutherford Appleton Laboratory* – ISIS, em Didcot, Reino Unido. Os nêutrons produzidos no ISIS originam-se do processo de fragmentação (*spallation*) em que um alvo composto por metal pesado (tungstênio) é bombardeado com pulsos de prótons altamente energéticos, gerando, então, nêutrons a partir do núcleo dos átomos atingidos (VIOLANTE et al., 2007). O fluxo médio obtido da fonte foi de $3{,}08.10^{4}$ n/cm²/s para energias acima de 10 MeV. A configuração do experimento montada no interior da câmara de irradiação VESUVIO no ISIS está representada pela Figura 52.

Figura 52 Experimento montado (o segundo da direita para a esquerda) na câmara de irradiação VESUVIO no ISIS. O DUT é a placa que está na vertical.

5.1.4 Resultados do Teste de *Single Event Effects*

O projeto do DUT resultou na ocupação de 94% dos recursos globais disponíveis no chip SmartFusion A2F200-FG484. Necessário observar, conforme já mencionado, que o ARM Cortex-M3 e o FPGA foram configurados para operar a 10 MHz enquanto que os blocos analógicos foram configurados para operar a 2,5 MHz. Sem considerar as interrupções sofridas pela cópia implementada em software, observou-se um atraso de aproximadamente 2 ms entre as saídas do processador e as saídas do FPGA.

O dispositivo foi exposto a um feixe de nêutrons com fluxo médio de $3{,}08.10^{4}$ n/cm²/s por um lapso temporal de vinte e quatro horas. Durante esse período, foram realizadas medições em tempo real para aferir a confiabilidade do FPGA SmartFusion no contexto de SEEs causados por nêutrons.

No que diz respeito aos conversores analógico-digital, observou-se uma seção de choque média de $8{,}18.10^{-5}$ cm² para o conversor "ADC0" e de $7{,}35.10^{-5}$ cm² para o conversor "ADC1", esses valores estão apresentados na Tabela 2. Imperioso notar que tais valores baseiam-se em todas as amostras – valores convertidos pelos conversores analógico-digital – gravadas, incluindo amostras com SEUs e possíveis rajadas de erros, em tradução livre do inglês *burst of errors*. As figuras 53 e 54 ilustram exemplos de amostras sem (*fault-free*) e com erros (*faulty*).

Tabela 2 Resultados obtidos para os conversores analógico-digital no experimento de SEEs

Tempo (h)	**Número de amostras**	**Amostras com erros (%)**		**Fluxo (n/cm²/s)**	**Seção de choque (cm²)**	
		ADC0	**ADC1**		**ADC0**	**ADC1**
06:00	399492	1,69	2,35	$3{,}07.10^{4}$	$5{,}52.10^{-5}$	$7{,}65.10^{-5}$
12:00	676136	2,93	2,22	$3{,}06.10^{4}$	$9{,}58.10^{-5}$	$7{,}25.10^{-5}$
18:00	413746	2,65	2,19	$3{,}08.10^{4}$	$8{,}61.10^{-5}$	$7{,}11.10^{-5}$
24:00	329319	2,79	2,28	$3{,}09.10^{4}$	$9{,}03.10^{-5}$	$7{,}38.10^{-5}$
Média				$3{,}08.10^{4}$	$8{,}18.10^{-5}$	$7{,}35.10^{-5}$
Desvio padrão				$0{,}01.10^{4}$	$1{,}96.10^{-5}$	$1{,}28.10^{-5}$

Em razão do projeto baseado nos conceitos de redundância dupla e diversificada, observou-se que a cópia que fez uso do ADC1, controlado pelo, FPGA apresentou um comportamento mais regular do que a cópia que utilizou o ADC0, controlada pelo ARM Cortex-M3. Uma justificativa para esse comportamento consiste no fato de que a aquisição contínua por parte do FPGA cria um cenário de sobreamostragem, tradução literal do termo inglês *oversampling*, o que não ocorre com a cópia controlada pelo processador.

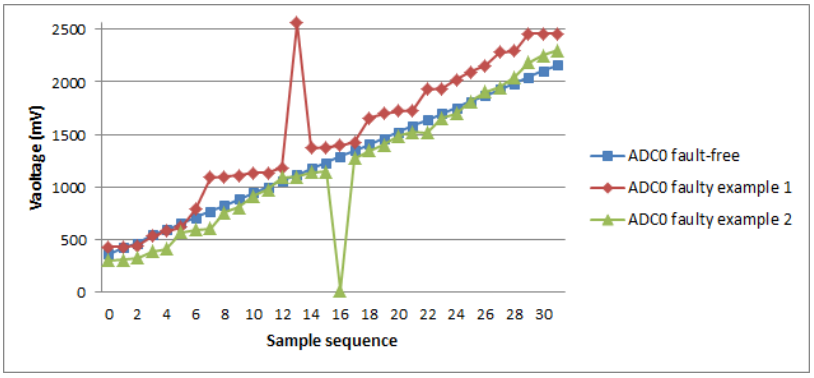

Figura 53 Exemplo de amostras obtidas do ADC0.

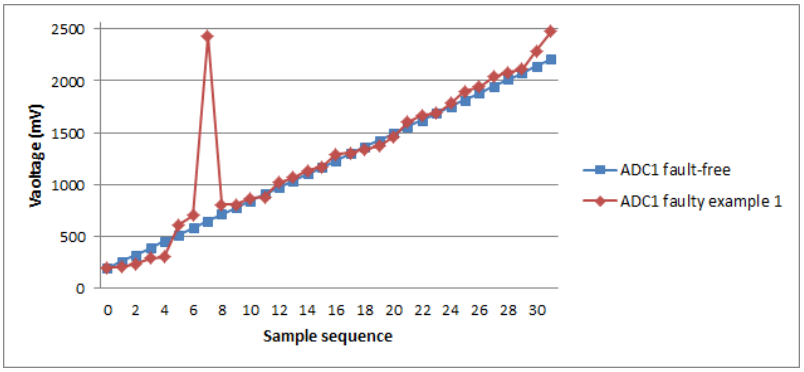

Figura 54 Exemplo de amostras obtidas do ADC1.

Das 1.818.693 amostras redundantes coletadas durante o teste, não foram observados erros simultâneos nos conversores analógico-digital. Tal situação reforça a conclusão de que, utilizando-se do conceito de redundância diversificada visando à detecção de erros, é possível detectar falhas nos caminhos de dados diversificados dos conversores analógico-digital. Pode-se afirmar, ainda, que o uso desse conceito em conjunto com um esquema de redundância modular tripla em FPGAs é valido na persecução da mitigação erros uma vez que a não obtenção de erros simultâneos reduz a probabilidade de que o votador de maioria forneça uma saída incorreta.

Quando investigadas topologias de conversores analógico-digital, pode-se aferir a existência de arquiteturas mais robustas à radiação. Pode-se citar, como exemplo, a arquitetura sigma-delta ($\Sigma\Delta$), a qual se provou ter um alto nível de tolerância à radiação (CORTES et al., 2002). Contudo, os conversores analógico-digital do FPGA SmartFusion são compostos por uma arquitetura de registrador de aproximação sucessiva (*Successive Approximation Register* – SAR) com capacitores chaveados *(switched-capacitor*), sendo esses ilustrados através da Figura 55. Tais capacitores são baseados no processo de redistribuição

de carga (MICROSEMI, 2011d) e possuem uma parte digital expressiva que pode ser facilmente afetada por SEUs.

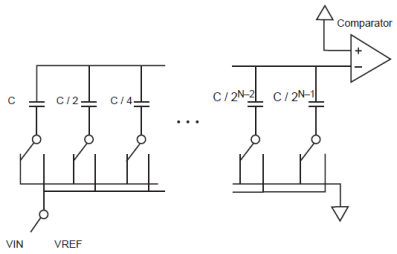

Figura 55 Ilustração de um arranjo de capacitores chaveados (MICROSEMI, 2011d).

Desse modo, observa-se a existência de duas principais possibilidades para a ocorrência de SEUs nos conversores análogico-digital do SmartFusion. A primeira possibilidade consiste, basicamente, na ocorrência de SEUs na lógica de controle ou SETs no comparador de um conversor analógico-digital do tipo SAR, o qual é baseado em um conjunto de capacitores, uma lógica digital de controle, um comparador e um circuito de amostra e espera (*sample and hold circuit*) que é responsável por adquirir uma tensão de entrada. A outra possibilidade está relacionada ao arranjo de capacitores chaveados e consiste no fato de que, se uma chave trocar temporariamente o seu estado (aberta ou fechada), também haverá modificação na capacitância equivalente do arranjo, ocorrendo, desse modo, um processo de redistribuição de carga entre cada parte do arranjo (BALEN et al., 2011b) que afetará o valor final.

Com relação aos circuitos digitais complementares implementados, observou-se a ocorrência de nove SEUs, seis MBUs e cinco rajadas de erros (*burst of errors*) nos registradores de deslocamento. Considerando que uma transmissão serial entre o DUT e a placa de controle leva 880 ns para ser completada, tem-se que as rajadas de erros podem ter sua origem na ocorrência de um SET ou um SEU na lógica da máquina de estados que realiza a serialização via FPGA ou em razão de erros nos blocos de saída do SmartFusion, como registradores e *buffers*, por exemplo.

A Figura 56 ilustra o modo como os registradores de deslocamento foram implementados em três níveis de abstração diferentes. A Figura 56(a) ilustra os registradores em nível de um diagrama de blocos. A Figura 56(b) ilustra como a ferramenta de síntese implementou cada instância dos registradores de deslocamento. A Figura 56(c) ilustra a arquitetura de um *VersaTile*, unidade básica em que cada bloco da Figura 56(b) é

implementado. Nesse caso, pode-se notar, através da análise da estrutura de um *VersaTile*, que, caso ocorra um SET em uma das suas instâncias, o estado de uma chave ou multiplexador poderá mudar, levando à geração de um SEU em um dos registradores de deslocamento.

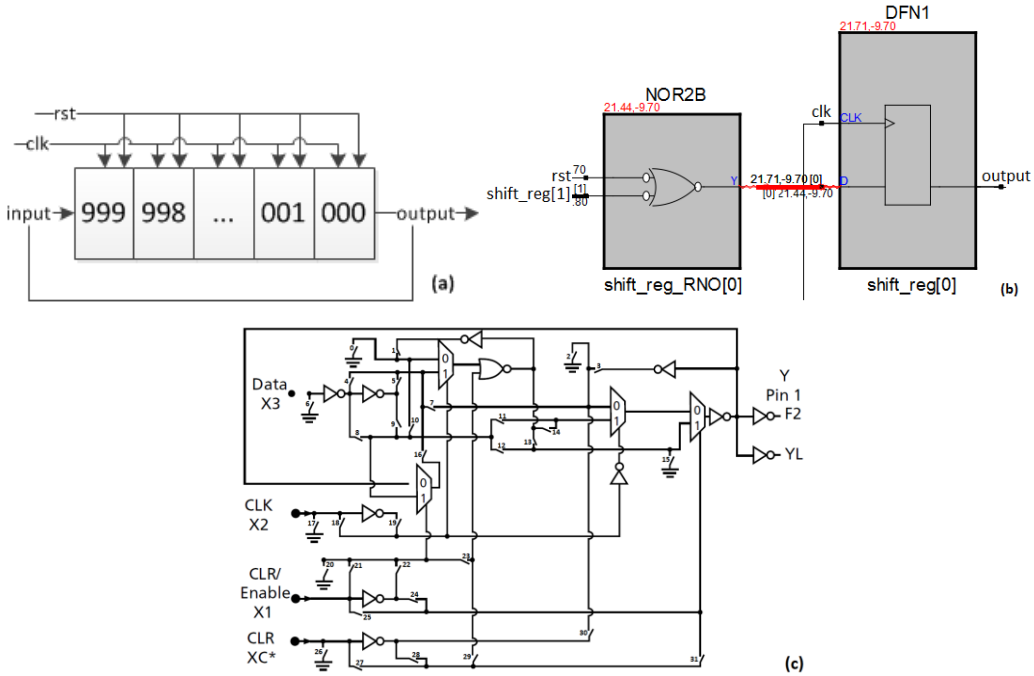

Figura 56 (a) Esquemático dos registradores de deslocamento implementados. (b) Como a ferramenta sintetiza cada instância de (a). (c) Arquitetura de um *VersaTile* (MICROSEMI, 2010).

5.2 Estudo de Caso II: Caracterização de um Esquema TMR Diversificado sob Radiação em um FPGA Spartan-6

O segundo estudo de caso reporta-se à análise das taxas de erros de uma arquitetura com aplicação específica desenvolvida, composta por um esquema baseado nos conceitos de redundância modular tripla e diversidade de projeto quando implementados em um FPGA da família Spartan-6, modelo XC6SLX45, da empresa Xilinx.

5.2.1 Arquitetura de Teste Desenvolvida

Para a realização dos testes, desenvolveu-se uma arquitetura cuja função principal é a de realizar a multiplicação de matrizes quadradas (8 x 8) compostas por valores com o tamanho de quatro bits.

A arquitetura foi, então, implementada com um esquema de tolerância a falhas baseado nos conceitos de redundância modular tripla (TMR) e redundância diversificada (DDR), ou seja, um TMR diversificado (*Diversity TMR* – DTMR). As cópias redundantes consistem em uma multiplicação de matrizes com *pipeline* de quatro estágios implementada através de uma máquina de estados, uma multiplicação de matrizes totalmente combinacional e uma multiplicação de matrizes implementada em *software* e embarcado no *soft-core* miniMIPS. Cada uma das cópias redundantes e o TMR possuem votadores de maioria em suas saídas. Por fim, o sistema conecta-se a uma interface de transmissão de dados. Essa sistemática é ilustrada na Figura 57. Todas as cópias foram implementadas na linguagem de descrição de hardware VHDL.

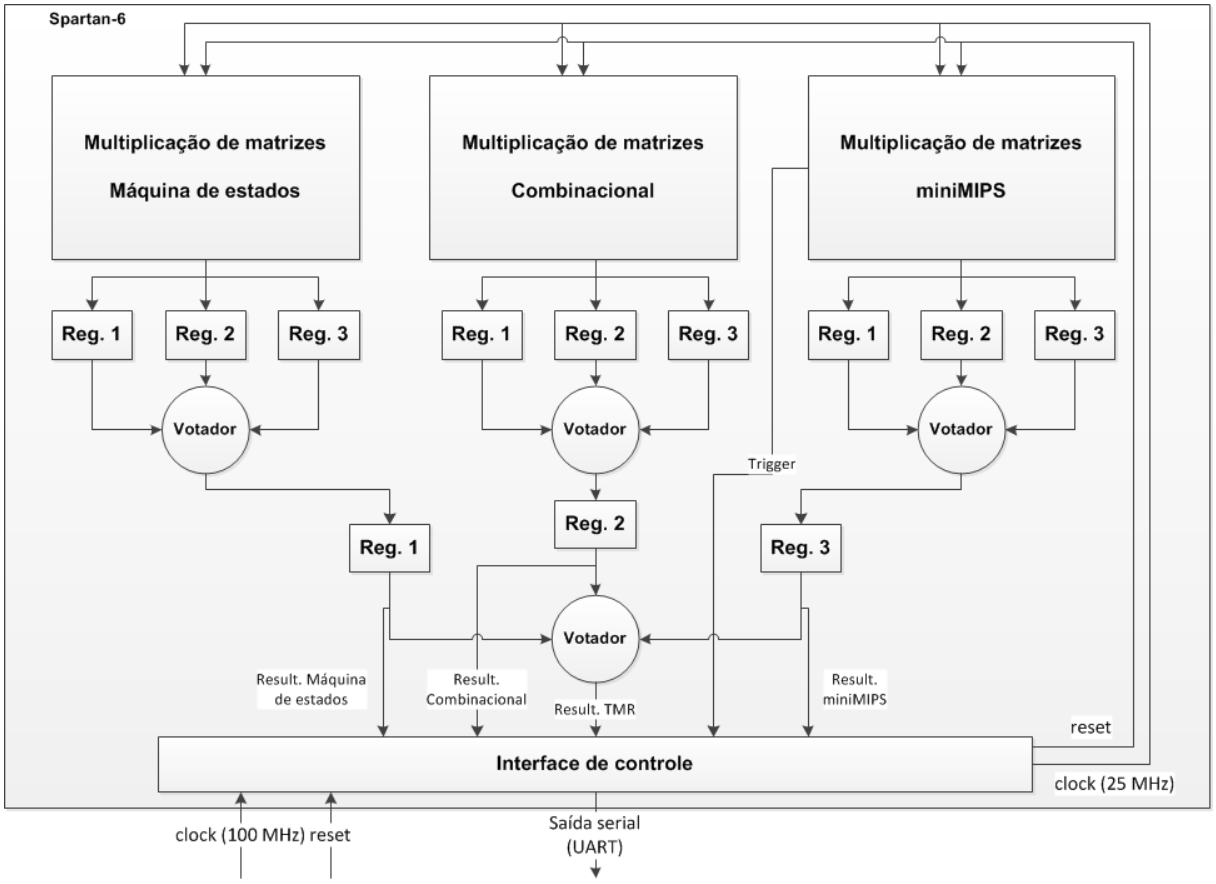

Figura 57 Esquemático da arquitetura de multiplicação de matrizes com DTMR desenvolvida. Os registradores são síncronos, porém os seus sinais de relógio (25 MHz) não foram ilustrado na figura com o objetivo de dar mais clareza a ela.

Na sequência, fornece-se à interface de controle um sinal de relógio de 100 MHz e um sinal de *reset* e esta, por sua vez, fornece à arquitetura DTMR um sinal de relógio de 25 MHz e um sinal de *reset* secundário.

A operação de multiplicação (A x B = C) realiza-se, então, com os seguintes valores estáticos salvos em memória: a matriz A possui todas as suas linha iguais (valores "[1, 4, 8, 8, 8, 8, 4, 1]") e a matriz B é composta de todos os seus elementos com o valor "1". Com isso, todos os elementos da matriz resposta C possuem o valor "42". O valor final de cada cópia redundante e, consequentemente, da arquitetura implementada consiste no somatório de todos os elementos da matriz resposta (valor "2688"). Todos os sinais foram implementados com o tipo *std_logic_vector*.

Cada uma das operações de multiplicação é feita em 255 ns na cópia totalmente combinacional, em 20,8 μs na cópia via máquina de estados com *pipeline* e em 1,5 ms na cópia via miniMIPS.

Composta por uma máquina de estados, uma memória no formato de uma fila (do acrônico em inglês *First In First Out* – FIFO) e por um módulo de comunicação UART, a interface de controle é responsável por realizar a aquisição dos dados da arquitetura DTMR e enviá-los a um computador via barramento UART.

A máquina de estados da interface de controle segue a seguinte sequência: no primeiro estado, todos os sinais sofrem um *reset*, inclusive os da arquitetura DTMR. No segundo estado, um contador de ciclos aguarda o sinal *trigger* chegar ao nível lógico um, porque geralmente encontra-se em nível lógico zero, indicando o fim da execução das três cópias redundantes (o *soft-core* miniMIPS é o mais demorado e, por isso, é utilizado como referência). Na hipótese de o contador de ciclos atingir o valor referente a 3 ms, gera-se um código de erro sinalizando que o tempo de execução padrão – 1,5 ms – foi ultrapassado (*timeout*) e a máquina de estados é direcionada para o quarto estado. Não havendo *timeout*, inicia-se o terceiro estado, no qual os quatro valores obtidos – três das cópias redundantes e um do votador final – são verificados e a cada um deles é associado um código de erro distinto para que, havendo alguma inconsistência, seja sinalizado o valor incorreto. Assim, existindo algum valor incorreto, forma-se um pacote de dados para transmissão no formato "código de erro | resultado miniMIPS | resultado combinacional | resultado máquina de estados | resultado final" e, então, a máquina de estados direciona-se para o quinto estado. Não havendo valores incorretos, um pacote de dados contendo o valor "85" é enviado apenas para indicar que o sistema está operando normalmente e, consequentemente, a máquina de estados retorna para o primeiro estado. No quarto estado, forma-se um pacote de dados com o código de erro de *timeout* e todos os outros dados com valor zero, o qual é enviado para a fila de transmissão do barramento UART e, consequentemente, a máquina de estados retorna ao primeiro estado. Por derradeiro, no quinto estado, tem-se que o pacote de dados formado no

terceiro estado é remetido à fila de transmissão do barramento UART e, após o envio, a máquina de estados retorna ao primeiro estado.

5.2.2 Montagem do Teste

A configuração do teste é dada pela utilização do DUT e de um computador, ambos conectados ponto-a-ponto via interface USB, sendo que uma das conexões tem a função de programar o dispositivo e a outra de realizar a comunicação via módulo USB-UART embarcado na placa Atlys. A alimentação da placa dá-se através de um conector de energia dedicado e ambas as conexões USB são realizadas através de cabos extensores, cada qual contendo um amplificador de sinal em um das suas extremidades, como ilustra a Figura 58.

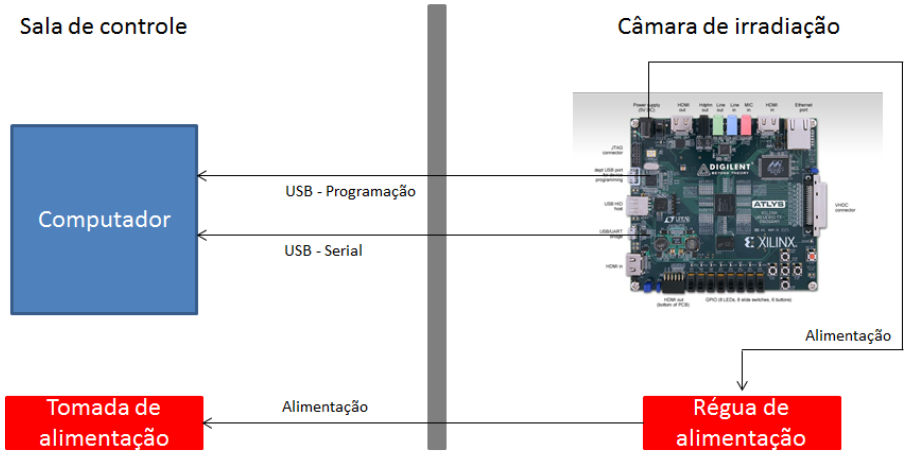

Figura 58 Organização do teste de SEEs na arquitetura DTMR embarcada no FPGA Spartan-6.

O controle do experimento é automatizado e é realizado através de um arquivo de lote, mais conhecido por *batch script* ou arquivo com extensão *.bat*, que é executado durante o experimento no computador em que o DUT está conectado. O *batch script* possui um laço – que corresponde a uma estrutura de programação mais conhecida pela expressão inglesa *loop* – que executa duas operações, a reprogramação e a aquisição dos dados do FPGA.

Dentro do laço do batch script, o primeiro comando a ser executado consiste na operação de reprogramação do dispositivo, que é realizada através de um comando que invoca a ferramenta de configuração iMPACT. Com o mesmo comando, é passado como argumento outro arquivo *batch script*, agora com extensão *.cmd*, contendo informações como o nome do arquivo de projeto da ferramenta para o FPGA Spartan-6 em uso, o modo de configuração do

dispositivo (*boundary scan*) e o arquivo contendo a configuração do dispositivo (extensão *.bit*).

A chamada ao software que realiza a operação de aquisição dos dados provenientes do FPGA é a segunda operação a ser executada no laço do *batch script* principal, sendo implementado na linguagem de programação C e ao qual são passados dois argumentos. O primeiro argumento consiste no identificador da porta serial – uma porta USB que é identificada como serial através do uso de um software de configuração, o *driver* – em que a placa Atlys está conectada. O segundo argumento, por sua vez, consiste no tempo máximo medido em segundos que o software irá guardar o recebimento de uma falha, o qual variou entre dez minutos até duas horas durante a realização do experimento.

Observa-se, de modo simplificado, que a implementação do software obedece à seguinte lógica: inicialmente, cria-se um arquivo para gravar as ações realizadas pelo software e os dados recebidos por ele; a validade dos argumentos é, então, verificada e, caso haja alguma inconsistência nos dados, gera-se uma mensagem indicando a ocorrência de algum erro nos argumentos e a execução do software é abortada. Não sendo observada qualquer inconsistência, é estabelecida a conexão do software com a porta serial indicada. Se houver algum erro nesta conexão, tal como porta em uso ou porta não identificada, uma mensagem de erro é gerada e a execução do software é abortada. Na hipótese de todos os comandos serem realizados com sucesso, tem-se que os dados provenientes do FPGA são armazenados.

O FPGA envia dados em três ocasiões: quando houver um valor incorreto na arquitetura DTMR, quando houver um erro de *timeout* ou quando o seu funcionamento estiver normal. Nas duas primeiras situações, o software irá aguardar até o término do tempo em segundos indicado no segundo argumento da sua chamada e, caso seja atingido esse tempo, o que indica que não houve nenhum erro no período de tempo, uma mensagem é gerada e a execução do software é abortada. Nos três casos, uma mensagem indicando a ocorrência de um erro de comunicação é gerada se nenhum dado for recebido dentro do tempo predeterminado e a execução do software é abortada.

Imperioso destacar dois pontos a respeito do *setup* do experimento, quais sejam: o software somente grava pacotes com dados incorretos ou mensagens de erros e que, sempre que o software é abortado, reinicia-se o *loop* do *batch script*, o que implica na reprogramação do dispositivo e na posterior reexecução do software de aquisição de dados.

Do mesmo modo com que foi realizado o experimento de SEEs com o SmartFusion, o teste na arquitetura DTMR foi executado no Rutherford Appleton Laboratory – ISIS, em

Didcot, Reino Unido. Nessa ocasião, o fluxo médio obtido da fonte foi de $4{,}29.10^4$ n/cm²/s para energias acima de 10 MeV. A Figura 59 ilustra a configuração do experimento montada dentro da câmara de irradiação VESUVIO no ISIS.

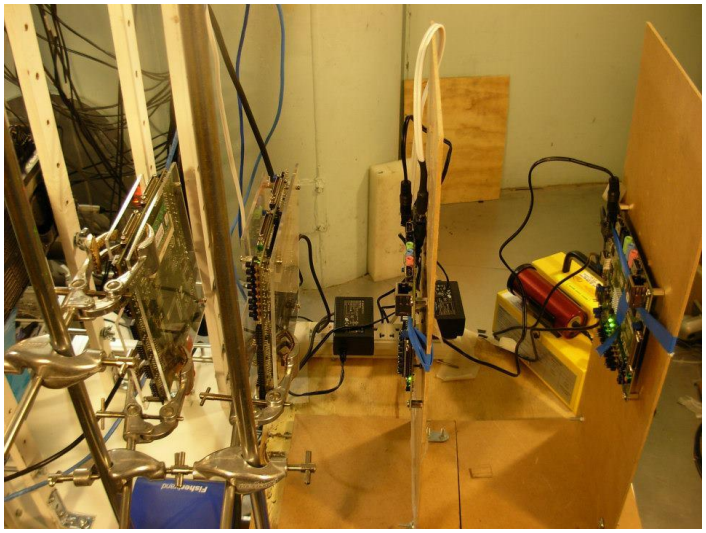

Figura 59 Experimento montado (o primeiro da direita para a esquerda) na câmara de irradiação VESUVIO no ISIS.

5.2.3 Resultados do Teste

O projeto do DUT resultou em 90% de ocupação dos *slices* disponíveis no FPGA Spartan-6. Em relação especificamente às LUTs, tem-se que 69% foram ocupadas. Em razão da impossibilidade de sintetizar todo o projeto DTMR apenas em blocos lógicos configuráveis, 13% dos blocos DSP48A1 foram utilizados no soft-core miniMIPS.

No que diz respeito à ocupação das LUTs por cada uma das cópias redundantes, tem-se que a implementação via máquina de estados com pipeline ocupou 10,78%, que a combinacional ocupou 52,12% e que a utilização do *soft-core* miniMIPS ocupou 36,73%. O módulo de controle utilizou 0,35% das LUTs ocupadas.

A análise e a consequente aquisição dos dados foram realizadas em tempo real para fins de aferir a confiabilidade da arquitetura DTMR implementada no FPGA Spartan-6 no contexto de SEEs causados por nêutrons. O dispositivo foi exposto a um feixe de nêutrons com um fluxo médio de $4{,}29.10^4$ n/cm²/s (desvio padrão $0{,}82.10^4$ n/cm²/s) por um período aproximado de setenta e duas horas.

Realizado o teste, observou-se a ocorrência de cinco erros na cópia redundante implementada via máquina de estados com *pipeline*, quatorze na cópia combinacional, oito no

soft-core miniMIPS e nenhum erro na saída da arquitetura DTMR. A partir desses resultados, é importante notar que a sensibilidade das cópias redundantes seguiu uma tendência proporcional às suas dimensões. Não foram observados erros de *timeout*. Três erros foram observados no módulo de controle através da aquisição de códigos de erros que não estavam previstos no projeto. O gráfico da Figura 60 ilustra os resultados obtidos no experimento para cada cópia redundante e para a arquitetura como um todo em função da seção de choque.

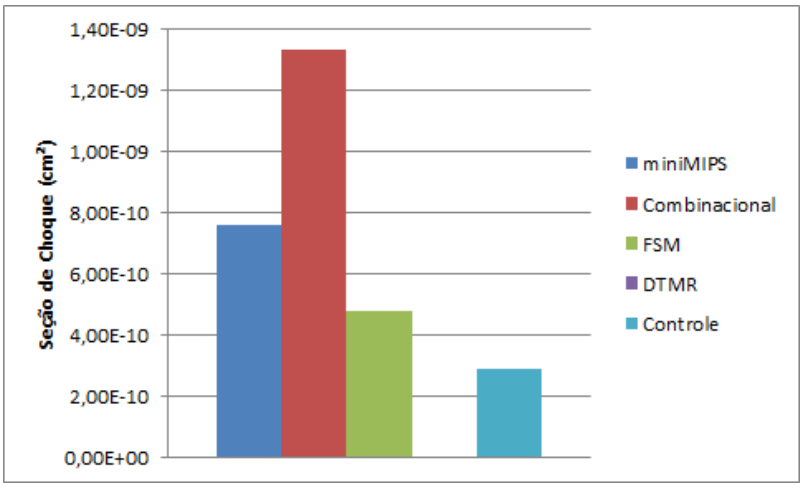

Figura 60 Seção de choque observada em cada bloco funcional da arquitetura DTMR durante o experimento de SEEs.

A possível ocorrência de muitos mascaramentos de falhas em razão da complexidade dos circuitos implementados pode ser uma das justificativas para o baixo número de erros observados – aproximadamente um erro a cada duas horas e vinte e quatro minutos. Paralelamente a este estudo de caso, foi realizado um experimento estático no mesmo Spartan-6 (placa Atlys) em que se obteve, em média, um erro a cada cinco minutos. De acordo com Xilinx (2011b), fazem-se necessários de dez a cem inversões de bits para que uma falha funcional seja realmente observada em um FPGA. Com isso, assumindo-se que seja necessária a ocorrência de trinta inversões de bits para que um erro seja observado e, ainda, que um erro se manifesta a cada cinco minutos, fazem-se necessárias duas horas e meia para que uma falha funcional seja observada, tempo semelhante ao observado no presente estudo de caso.

Imperioso destacar, novamente, que a adoção de um projeto diversitário tem como finalidade reduzir a probabilidade de que falhas múltiplas afetem diferentes blocos em razão da implementação de diferentes arquiteturas nas cópias de um sistema redundante, o que ocorre porque as cópias podem apresentar diferentes níveis de tolerância associados às

diferentes fontes e mecanismos de geração de falhas. Em função disso, observou-se que o sistema apresentou uma tolerância a falhas de 100%, uma vez que nenhum erro foi observado na saída da arquitetura DTMR.

6 CONCLUSÕES

Este trabalho consiste de um estudo acerca dos efeitos da radiação em circuitos programáveis. Inicialmente foi realizada uma revisão teórica sobre as origens da radiação espacial e os seus efeitos em circuitos integrados. Posteriormente, o estado-da-arte no que diz respeito às técnicas de detecção e mitigação de falhas baseadas em redundância e aplicáveis a sistemas sujeitos à radiação foi apresentado e a metodologia de caracterização de circuitos programáveis adotada foi definida. Desse modo, os três primeiros capítulos contribuem com uma revisão abrangente sobre o tema. Além disso, os capítulos em questão podem servir como referência a estudantes e pesquisadores que objetivam ingressar na área de tolerância a falhas no que diz respeito à interação da radiação com circuitos integrados eletrônicos e as técnicas de detecção e mitigação de falhas baseadas em redundância em nível de sistema existentes. O capítulo quatro apresentou de forma genérica como um FPGA ou SoC é organizado e os dispositivos físicos utilizados como objeto de experimentação.

O capítulo cinco abordou na sua primeira subseção a caracterização dos principais blocos funcionais do FPGA de sinais mistos comercial SmartFusion sob radiação através do uso da técnica de Redundância Diversificada. Dispositivos deste tipo são uma alternativa de baixo custo para projetos de sinais mistos, visto que a integração de diversos blocos funcionais em um só dispositivo pode reduzir a área ocupada por um sistema, bem como a sua complexidade. Foram analisados os efeitos de dose total ionizante acumulada e de eventos transitórios causados por nêutrons. Desse modo, e devido ao fato deste trabalho ser o primeiro a adotar o SmartFusion como estudo de caso, os resultados apresentados nesta dissertação podem servir como referência para projetistas de sistemas que possam vir a cogitar a adoção de um dispositivo programável de sinais mistos em seus projetos.

Na segunda subseção do capítulo cinco abordou-se o teste prático de uma arquitetura redundante e diversificada, ou seja, que faz uso dos conceitos de Redundância Modular Tripla e Diversidade de Projeto. A adoção de uma abordagem redundante e diversificada em projetos que requerem um alto grau de confiabilidade é uma opção atrativa pelo fato de que quando as cópias de uma implementação em um sistema redundante são construídas com diferentes arquiteturas, a probabilidade de falhas múltiplas afetarem diferentes blocos é reduzida, uma vez que cada cópia pode apresentar diferentes níveis de tolerância associados às diferentes fontes e mecanismos de geração de falhas. Não foram encontrados na literatura dados de testes práticos realizados em arquiteturas semelhantes. Por conta disso, este trabalho torna-se

uma alternativa para projetistas que necessitam de informações acerca do comportamento de um sistema redundante e diversificado na prática.

Os trabalhos relacionados a esta dissertação geraram três publicações em anais de eventos (TAMBARA et al., 2011; TAMBARA et al., 2012a; TAMBARA et al., 2012b).

Embora os trabalhos realizados nesta dissertação tenham agregado resultados interessantes à área de tolerância a falhas causadas pela radiação em circuitos programáveis, ainda há muito a ser investigado. No que diz respeito ao FPGA SmartFusion é preciso, principalmente, caracterizar os conversores de analógico-digital para dose total ionizante. A respeito da arquitetura redundante e diversificada, ainda é necessário caracterizá-la no contexto de dose total ionizante. Outros experimentos podem ser realizados com o objetivo de obter novos dados e refinar os já adquiridos e expostos neste trabalho. Simulações elétricas da arquitetura dos conversores analógico-digital embarcados no SmartFusion têm sido realizadas e os seus resultados serão apresentados em trabalhos futuros. Injeções de falhas na arquitetura redundante e diversificada estão sendo planejadas e é a próxima etapa a ser realiza como continuação deste trabalho.

REFERÊNCIAS

ALTERA. **Cyclone V FPGAs**. 2012. Disponível em: <www.altera.com>. Acesso em: 30 jan. 2013.

ANGHEL, A.; ALEXANDRESCU, D.; NICOLAIDIS, M. Evaluation of a Soft Error Tolerance Technique Based on Time and or Hardware Redundancy. In: IEEE INTEGRATED CIRCUITS AND SYSTEMS DESIGN (SBCCI), 13., 2000, Manaus. **Proceedings**… [s. l.]: IEEE Computer Society, 2000. p. 237-242.

ASHRAF, R. A. et al. Design-for-Diversity for Improved Fault-Tolerance of TMR Systems on FPGAs. In: INTERNATIONAL CONFERENCE ON RECONFIGURABLE COMPUTING AND FPGAS, 2011, Cancun. **Proceedings...** [s. 1.]: IEEE, 2011. p. 99-104.

AVIZIENIS, A.; CHEN, L. On the Implementation of N-Version Programming for Software Fault Tolerance During Execution. In: INTERNATIONAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE (COMPSAC), 1977, [s. l.]. **Proceedings...** [s. 1.]: [s. n.], 1977. p. 149-155.

AVIZIENIS, A.; KELLY, J. P. J. Fault Tolerance by Design Diversity: Concepts and Experiments. **Computer**, Los Alamitos, v. 17, n. 8, p. 67-80, Aug. 1984.

BALEN, T. R. et al. TID in a Switched-Capacitor FPAA: Degradation and Partial Inactivity Windows Due to Compensating Effects in MOS Transistors. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 58, n. 6, p. 2883–2889, Dec. 2011a.

BALEN, T. R. et al. Investigating the Effects of Transient Faults in Programmable Capacitor Arrays. In: LATIN AMERICAN TEST WORKSHOP, 12., 2011, Porto de Galinhas. **Proceedings…** [s. 1.]: IEEE, 2011b. p. 1-6.

BATTEZZATI, N. et al. Methodologies to Study Frequency-Dependent Single Event Effects Sensitivity in Flash-Based FPGAs. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 56, n. 6, p. 3534–3541, Dec. 2009.

BAUMANN, R. Soft Errors in Advanced Semiconductor Devices-part I: The Three Radiation Sources. **IEEE Transactions on Device and Materials Reliability**, [s. l.], v. 1, n. 1, p. 17-22, Mar. 2001.

BAUMANN, R. Soft Errors in Advanced Semiconductor Devices. **IEEE Design & Test of Computers**, Los Alamitos, v. 22, n. 3, p. 258-266, Jun. 2005a.

BAUMANN, R. Radiation-induced Soft Errors in Advanced Semiconductor Technologies. **IEEE Transactions on Device and Materials Reliability**, [s. l.], v. 5, n. 3, p. 305-316, Sept. 2005b.

BELLATO, M. et al. Evaluating the Effects of SEUs Affecting the Configuration Memory of an SRAM-based FPGA. In: DESIGN, AUTOMATION AND TEST IN EUROPE CONFERENCE (DATE), 2004, Paris. **Proceedings…** [s. l.]: IEEE Computer Society, 2004. p. 584-589.

BORKAR, S. Designing Reliable Systems from Unreliable Components: The Challenges of Transistor Variability and Degradation. **IEEE Micro**, Los Alamitos, v. 25, n. 6, p. 10-16, Nov./Dec. 2005.

BORGES, G. M. et al. Diversity TMR: Proof of Concept in a Mixed-Signal Case. In: IEEE LATIN AMERICAN TEST WORKSHOP, 11., 2010, Pule del Este. **Proceedings...** [s. 1.]: IEEE, 2010a. p. 1-6.

BORGES, G. M. et al. Evaluating the Effectiveness of a Mixed-Signal TMR Scheme Based on Design Diversity. In: SYMPOSIUM ON INTEGRATED CIRCUITS AND SYSTEM DESIGN, 23., 2010, São Paulo. **Proceedings…** [s. l.]: ACM, 2010b. p. 134-139.

BOUDENOT, J. C. Radiation Space Environment. In. VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007. p. 1-9.

CADENCE. Cadence Design Systems. **Mixed Signal: Why the Sudden Attention?** 2010. Disponível em: <www.cadence.com/Community/blogs/di/archive/2010/05/24/mixed-signal-why-the-sudden-jump-in-attention.aspx>. Acesso em: 30 jan. 2013.

CHAU, S. N.; SMITH, J.; TAI, T. A Design-Diversity Based Fault-Tolerant COTS Avionics Bus Network. In: INTERNATIONAL SYMPOSIUM ON DEPENDABLE COMPUTING, 2001, Seoul. **Proceedings…** [s. l.]: IEEE Computer Society, 2001. p. 35-42.

CINARELLI, D.; TORTORA, P. TT&C System for the ALMASat-EO Microsatellite Platform. In: IEEE AESS EUROPEAN CONFERENCE ON SATELLITE TELECOMMUNICATIONS, 1., 2012, Rome. **Proceedings…** [s. 1.]: IEEE, 2012. p. 1-6.

COOK, K. L. B. The ITAR and You – What You Need to Know about the International Traffic in Arms Regulations. In: IEEE AEROSPACE CONFERENCE, 2010, Big Sky. **Proceedings…** [s. l.]: IEEE, 2010. p. 1-12.

CYPRESS. **Programmable System-on-Chip**. 2012. Disponível em: <www.cypress.com>. Acesso em: 30 jan. 2013.

CLAEYS, C.; SIMOEN, E. **Radiation Effects in Advanced Semiconductor Materials and Devices**. Berlin: Springer, 2002.

CORTES, F. P. et al. A $\Sigma\Delta$ A/D Converter Insensitive to SEU effects. In: INTERNATIONAL ON-LINE TESTING WORKSHOP, 8., 2002, Isle of Bendor. **Proceedings…** [s. l.]: IEEE Computer Society, 2002. p. 89-93.

DODD, P. E.; SEXTON, F. W. Critical Charge Concepts for CMOS SRAMs. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 42, n. 6, p. 1764-1771, Dec. 1995.

DODD, P. E. et al. Impact of Technology Trends on SEU in CMOS SRAMs. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 43, n. 6, p. 2797-2804, Dec. 1996.

DODD, P. E. et al. Neutron-induced Soft Errors, Latchup, and Comparison of SER Test Methods for SRAM Technologies. In: INTERNATIONAL ELECTRON DEVICE MEETING, 2002, San Francisco. **Proceedings…** [s. l.]: IEEE, 2002. p. 333-336.

DODD, P. E.; MASSENGILL, L. W. Basic Mechanisms and Modeling of Single-Event Upset in Digital Microelectronics. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 50, n. 3, p. 583-602, June 2003.

DUPONT, E.; NICOLAIDIS, M.; ROHR, P. Embedded Robustness IPs for Transient-error-free ICs. **IEEE Design & Test of Computers**, Los Alamitos, v. 19, n. 3, p. 54-68, May/June 2002.

DUZELLIER, S.; BERGER, G. Test Facilities for SEE and Dose Testing. In. VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007. p. 201-232.

DYER, C. S. et al. Observation of the Solar Particle Events of October and November 2003 from CREDO and MPTB. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 51, n. 6, p. 3388-3393, Dec. 2004.

ECOFFET, R. In-flight Anomalies on Electronic Devices. In. VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007. p. 31-68.

ELMENDORF, W. R. Fault-Tolerant Programming. In: INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING SYSTEMS, 1972, [s. 1.]. **Proceedings…** [s. 1.]: [s. n.], 1972. p. 79-83.

ENTRENA, L. et al. SET Emulation Considering Electrical Masking Effects. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 56, n. 4, p. 2021-2025, Aug. 2000.

EUROPEAN SPACE AGENCY (ESA). **The Radiation Design Handbook**. Noordwijk: European Space Agency, 1993.

FACCIO, F.; CERVELLI, G. Radiation-Induced Edge Effects in Deep Submicron CMOS Transistors. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 52, n. 6, p. 2413-2420, Dec. 2005.

FACCIO, F. Design Hardening Methodologies for ASICs. In. VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007. p. 143-160.

FERAIN, I.; COLINGE, C. A.; COLINGE, J.-P. Multigate Transistors as the Future of Classical Metal–Oxide–Semiconductor Field-Effect Transistors. **Nature**, Basingstoke, v. 479, n. 7372, p. 310-316, Nov. 2011.

FRANCO, F. J.; ZONG, Y.; AGAPITO, J. A. Inactivity Windows in Irradiated CMOS Analog Switches. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 53, n. 4, p. 1923–1930, Aug. 2006.

GANSSLE, J.; BARR, M. **Embedded Systems Dictionary**. Hong Kong: CMP Books, 2003.

GASIOT, G.; GIOT, D.; ROCHE, P. Alpha-Induced Multiple Cell Upsets in Standard and Radiation Hardened SRAMs Manufactured in a 65nm CMOS Technology. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 53, n. 6, p. 3479-3486, Dec. 2006.

GEORGIA STATE UNIVERSITY. **Cosmic Rays**. 1999. Disponível em: < hyperphysics.phy-astr.gsu.edu/HBASE/astro/cosmic.html>. Acesso em: 28 dez. 2012.

GOLOUBEVA, O. et al. **Software-Implemented Hardware Fault Tolerance**. New York: Springer, 2006.

GROSSO, M. et al. A Software-based Self-test Methodology for System Peripherals. In: IEEE EUROPEAN TEST SYMPOSIUM (ETS), 15., 2010, Praha. **Proceedings…** [s. l.]: IEEE TTTC, 2010. p. 195-200.

GUSSENHOVER, M. S.; MULLEN, E. G.; BRAUTIGAM, D. H. Improved Understanding of the Earth's Radiation Belts from the CRRES Satellite. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 43, n. 2, p. 353-368, Aug. 1996.

HIARI, O.; SADEH, W.; RAWASHDEH, O. Towards Single-Chip Diversity TMR for Automotive Applications. In: IEEE INTERNATIONAL ELECTRO/INFORMATION TECHNOLOGY, 2012, Indianapolis. **Proceedings…** [s. l.]: IEEE, 2012. p. 1-6.

HOUGHTON, A. D. **The Engineer's Error Coding Handbook**. London: Chapman & Hall, 1997.

HUGHES, R. C. Charge Carrier Transport Phenomena in Amorphous SiO_2: Direct Measurement of Mobility and Carrier Lifetime. **Physical Review Letters**, New York, v. 30, n. 26, p. 1333-1336, June 1973.

HSIEH, C. M.; MURLEY, P. C.; O'BRIEN, R. R. Dynamics of Charge Collection from Alpha-Particle Tracks in Integrated Circuits. In: IEEE INTERNATIONAL RELIABILITY PHYSICS SYMPOSIUM, 19., 1981, Las Vegas. **Proceedings…** [s. l.]: IEEE, 1981. p. 38-42.

INTERNATIONAL SOLID-STATE CIRCUITS CONFERENCE (ISSCC). **ISSCC 2011 Trends Report**. 2011. Disponível em: <isscc.org/doc/2011/2011_Trends.pdf>. Acesso em: 08 fev. 2013.

KASTENSMIDT, F. G. L. **Designing Single Event Upset Mitigation Technique for Large SRAM-based FPGA Components**. 2003. 157 p. Tese (Doutorado em Computação) – Programa de Pós-Graduação em Computação. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2003.

KASTENSMIDT, F.; CARRO, L.; REIS, R. **Fault-Tolerance Techniques for SRAM-based FPGAs**. Dordrecht: Springer, 2006.

KASTENSMIDT, F.; REIS, R. Fault Tolerance in Programmable Circuits. In. VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007. p. 161-181.

KASTENSMIDT, F. L. et al. TID in Flash-Based FPGA: Power Supply-Current Rise and Logic Function Mapping Effects in Propagation-Delay Degradation. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 58, n. 4, p. 1927-1934, Aug. 2011.

KATZ, R. et al. Radiation Effects on Current Field Programmable Technologies. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 44, n. 6, p. 1945-1956, Dec. 1997.

KUEN-JONG, L. et al. On-Chip SOC Test Platform Design Based on IEEE 1500 Standard. **IEEE Transactions on Very Large Scale Integration (VLSI) Systems**, New York, v. 18, n. 7, p. 1134-1139, July 2010.

LALA, J. H.; HARPER, R. E. Architectural Principles for Safety-Critical Real-Time Applications. **Proceedings of the IEEE**, New York, v. 82, n. 1, p. 25-40, Jan. 1994.

LECHNER, A.; RICHARDSON, A. Test of A/D Converters. In: HUERTAS, J. L. (Ed.). **Test and Design-for-Testability in Mixed-Signal Integrated Circuits**. Dordrecht: Kluwer Academic Publishers, 2004. p.73–98.

MICROSEMI. **Actel SmartFusion FPGA Fabric User's Guide**. 2010. Disponível em: <www.actel.com>. Acesso em: 03 nov. 2011.

MICROSEMI. **SmartFusion Customizable System-on-Chip (cSoC)**. 2011a. Disponível em: <www.actel.com>. Acesso em: 03 nov. 2011.

MICROSEMI. **Understanding Single Event Effects (SEEs) in FPGAs**. 2011b. Disponível em: <www.actel.com>. Acesso em: 03 nov. 2011.

MICROSEMI. **SmartFusion Microcontroller Subsystem User's Guide**. 2011c. Disponível em: <www.actel.com>. Acesso em: 03 nov. 2011.

MICROSEMI. **SmartFusion Programmable Analog User's Guide**. 2011d. Disponível em: <www.actel.com>. Acesso em: 03 nov. 2011.

MICROSEMI. **SmartFusion Evaluation Kit User's Guide**. 2011e. Disponível em: <www.actel.com>. Acesso em: 03 nov. 2011.

MICROSEMI. **SmartFusion cSoC**. 2012. Disponível em: <www.actel.com>. Acesso em: 30 jan. 2013.

MITRA, S.; SAXENA, N.; MCCLUSKEY, E. A Design Diversity Metric and Reliability Analysis for Redundant Systems. In: INTERNATIONAL TEST CONFERENCE (ITC), 1999, Atlantic City. **Proceedings…** [s. l.]: IEEE Computer Society, 1999. p. 662-671.

MITRA, S.; SAXENA, N.; MCCLUSKEY, E. Techniques for Estimation of Design Diversity for Combinational Logic Circuits. In: INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS, 2001, Goteborg. **Proceedings…** [s. l.]: IEEE Computer Society, 2001. p. 25-34.

MITRA, S.; SAXENA, N.; MCCLUSKEY, E. A Design Diversity Metric and Analysis of Redundant Systems. **IEEE Transactions on Computers**, Los Alamitos, v. 51, n. 5, p. 498-510, May 2002.

MITRA, S.; SAXENA, N.; MCCLUSKEY, E. Efficient Design Diversity Estimation for Combinational Circuits. **IEEE Transactions on Computers**, Los Alamitos, v. 53, n. 11, p. 1483-2004, Nov. 2004.

NICOLAIDIS, M. Time Redundancy Based Soft-error Tolerance to Rescue Nanometer Technologies. In: IEEE VLSI TEST SYMPOSIUM, 17., 1999, Dana Point. **Proceedings…** [s. l.]: IEEE Computer Society, 1999. p. 86-94.

NICOLAIDIS, M. Circuit-Level Soft-Error Mitigation. In. NICOLAIDIS, M. (Ed.). **Soft Errors in Modern Electronic Systems**. Dordrecht: Springer, 2011. p. 203-252.

NORMAND, E. Single Event Effects in Avionics. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 43, n. 2, p. 461-474, Apr. 1996.

O'BRYAN, M.; LABEL, K. Recent Radiation Damage and Single Event Effects Results for Candidate Spacecraft Electronics. In: IEEE NUCLEAR SPACE RADIATION EFFECTS CONFERENCE (NSREC), 2001, Vancouver. **Proceedings…** [s. l.]: IEEE NPSS, 2001. p. 82-99.

OLDHAM, T. R.; MCLEAN, F. B. Total Ionizing Dose Effects in MOS Oxides and Devices. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 50, n. 3, p. 483-499, June 2003.

PETERSON, W. W. **Error-Correcting Codes**. Cambridge: MIT, 1980.

PULLUM, L. L. **Software Fault Tolerance Techniques and Implementation**. Boston: Artech House, 2001.

RITER, R. Modeling and Testing a Critical Fault-Tolerant Multi-Process System. In: INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING, 25., 1995, Pasadena. **Proceedings…** [s. l.]: IEEE Computer Society, 1995. p. 516-521.

RODGER, C. J.; CLILVERD, M. A. Magnetospheric Physics: Hiss from the Chorus. **Nature**, Basingstoke, v. 452, n. 7183, p. 41-42, Mar. 2008.

SCHRIMPF, R. D. Radiation Effects in Microelectronics. In. VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007. p. 11-29.

SCHWANK, J. R. et al. Radiation Effects in MOS Oxides. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 55, n. 4, p. 1833-1853, Aug. 2008.

SHIVAKUMA, P. et al. Modeling the Effect of Technology Trends on the Soft Error Rate of Combinational Logic. In: INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS, 2002, Washington. **Proceedings…** [s. l.]: IEEE Computer Society, 2002. p. 389-398.

SNOW, E. H.; GROVE, S.; FITZGERALD, D. J. Effects of Ionizing Radiation on Oxidized Silicon Surfaces and Planar Devices. **Proceedings of the IEEE**, New York, v. 55, n. 7, p. 1168-1184, July 1967.

SRINIVASAN, S. et al. Toward Increasing FPGA Lifetime. **IEEE Transactions on Dependable and Secure Computing**, Los Alamitos, v. 5, n. 2, p. 115-127, Apr./June 2008.

STEFAN. Institut Jožef Stefan. **Understanding the Muon Lifetime Experiment**. 2001. Disponível em: <www-f9.ijs.si/~rok/sola/praktikum4/mioni/muonexp.html>. Acesso em: 28 dez. 2012.

TAMBARA, L. A. et al. TID in a Mixed-Signal System-on-Chip: Analog Components Analysis and Clock Frequency Influence in Propagation-Delay Degradation. In: IEEE RADIATION EFFECTS DATA WORKSHOP (REDW), 2011, Miami. **Proceedings…** [s. l.]: IEEE, 2011. p. 1-6.

TAMBARA, L. A. et al. Neutron-induced Single Event Effect in Mixed-Signal Flash-based FPGA. In: EUROPEAN CONFERENCE ON RADIATION AND ITS EFFECTS ON COMPONENTS AND SYSTEMS (RADECS), 13., 2012, Biarritz. **Proceedings…** [s. l.]: IEEE, 2012a. p. 1-5.

TAMBARA, L. A. et al. Total Ionizing Dose in a Mixed-Signal Flash-based FPGA. In: WORKSHOP ANUAL SOBRE OS EFEITOS DAS RADIAÇÕES IONIZANTES EM COMPONENTES ELETRÔNICOS E FOTÔNICOS DE USO AEROESPACIAL (WERICE), 2012, São José dos Campos. **Anais…** São José dos Campos: IEAv, 2012b. p. 82-87.

TAUR, Y. et al. CMOS Scaling Into the Nanometer Regime. **Proceedings of the IEEE**, New York, v. 85, n. 4, p. 486-504, Apr. 1997.

TSAO, C. H.; SILBERBERG, R.; LETAW, J. R. Cosmic Ray Heavy Ions at and Above 40,000 Feet. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 31, n. 6, p. 1183-1185, Dec. 1984.

VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007.

VELAZCO, R.; FAURE, F. Error Rate Prediction of Digital Architectures: Test Methodology and Tools. In. VELAZCO, R.; FOUILLAT, P.; REIS, R. (Ed.). **Radiation Effects on Embedded Systems**. Dordrecht: Springer, 2007. p. 233-258.

VIOLANTE, M. et al. A New Hardware/Software Platform and a New 1/E Neutron Source for Soft Error Studies: Testing FPGAs at the ISIS Facility. **IEEE Transactions on Nuclear Science**, Albuquerque, v. 54, n. 4, p. 1184-1189, Aug. 2007.

XILINX. **Triple Modular Redundancy Design Techniques for Virtex Series FPGA**. 2001. Disponível em: <www.cs.york.ac.uk/rts/docs/Xilinx-datasource-2003-q1/appnotes/xapp197.pdf>. Acesso em: 06 mar. 2013.

XILINX. **Spartan-6 FPGA DSP48A1 Slice**. 2009. Disponível em: <www.xilinx.com>. Acesso em: 26 fev. 2013.

XILINX. **Spartan-6 FPGA Configurable Logic Block**. 2010. Disponível em: <www. xilinx.com>. Acesso em: 26 fev. 2013.

XILINX. **Spartan-6 FPGA Block RAM Resources**. 2011a. Disponível em: <www. xilinx.com>. Acesso em: 26 fev. 2013.

XILINX. **Continuing Experiments of Atmospheric Neutron Effects on Deep Submicron Integrated Circuits**. 2011b. Disponível em: <www.xilinx.com>. Acesso em: 04 mar. 2013.

XILINX. **Zynq-7000 Extensible Processing Platform**. 2012. Disponível em: <www.xilinx.com/products/silicon-devices/soc/zynq-7000>. Acesso em: 30 jan. 2013.

WANG, F; AGRAWAL, V. D. Single Event Upset: An Embedded Tutorial. In: IEEE INTERNATIONAL CONFERENCE ON VLSI DESIGN, 21., 2008, Hyderabad. **Proceedings…** [s. l.]: IEEE Computer Society, 2008. p. 429-434.

WEAVER, H. T. et al. RAM Cell Recovery Mechanisms Following High-energy Ion Strikes. **IEEE Electron Device Letters**, Piscataway, v. 8, n. 1, p. 7-9, Jan. 1987.

ZHU, Q. et al. An Object-oriented Design Process for System-on-Chip Using UML. In: INTERNATIONAL SYMPOSIUM ON SYSTEM SYNTHESIS, 15., 2002, Kyoto. **Proceedings…** [s. l.]: ACM, 2002. p. 249-254.

ZIEGLER, J. F.; LANFORD, W. A. Effect of Cosmic Rays on Computer Memories. **Science**, [s. l.], v. 206, n. 4420, p. 776-788, Nov. 1979.

ZIEGLER, J. F. et al. IBM Experiments in Soft Fails in Computer Electronics (1978-1994). **IBM J. Research and Development**, Riverton, v. 40, n. 1, p. 3-18, Jan. 1996.

ZIEGLER, J. F.; PUCHNER, H. **SER – History, Trends and Challenges:** A Guide for Designing with Memory ICs. San Jose: Cypress Semiconductor, 2004.