Fault Mitigation in High-performance FPGA-based Safety-critical Systems in a Radiation Environment

Carlos Leong
1. Introduction
2. Physical Disturbances (PVTR-A variations)
3. Single Event Effects (SEE) and Rad Charact.
4. SEE Mitigation Techniques
5. Long Term Error (LTE) Mitigation Techniques
6. Standard Compliance
7. Avenues of Research
8. References
Motivation

- SRAM **FPGA-based robust design** (Xilinx™)
- High-performance, safety-critical applications, long lifetime products
- LP (Low-power) functional and test mode
- Tolerance to variability (PVT-R-A) (magnetics also?)
- Immunity system, adaptive system along product lifetime, each device delivering correct functionality with minimum power
- Use state-of-the-art FPGA vendor tools
- Standard compliance
- Markets: medical, automotive, aerospace, physics experiments (CERN, ITER)
- Focus: *start with aerospace, rad-tolerant using COTS*
2. Physical Disturbances

- Sources of Variability
  - Transient (short term)
    - P (Process)
    - V (power supply Voltage)
    - T (Temperature)
    - R (Radiation)
    - M (Magnetics?)
  - Permanent (long term)
    - A (Aging, including radiation-induced – TID)
3. Single Event Effects (SEE)

- **Soft error**
  - SET (Single Event Transient)
  - SEU (Single Event Upset)
  - SEFI (Single Event Functional Interrupt)
  - SBU (Single Bit Upset)
  - MBU (Multiple Bit Upset)
  - Recoverable Errors

- **Hard error**
  - SEL (Single Event Latch-Up)
  - SEB (Single Event Burnout)
  - SEGR (Single Event Gate Rupture)
  - Non-Recoverable Errors
Radiation-Induced Faults

**SOFT ERRORS - recoverable**

- **SINGLE EVENT TRANSIENT (SET):** peaks in combinational IC’s
- **SINGLE EVENT UPSET (SEU):** change of data in memory cells
  - **SINGLE BIT UPSET (SBU):** SEU that affects a single bit
  - **MULTIPLE BIT UPSET (MBU):** several simultaneous SBU’s
- **FUNCTIONAL INTERRUPTION (SEFI):** circuit became halted

**HARD ERRORS - unrecoverable**

- **SINGLE EVENT LATCH-UP (SEL):** parasitic thyristor trigger
- **SINGLE EVENT BURNOUT (SEB):** induced short circuit and subsequent burnout
- **SINGLE EVENT GATE RUPTURE (SEGR):** gate oxide destruction
Main concerns:

**Alpha Particles**: from packaging material natural decay

**Neutrons**: from cosmic high speed particles

Neutron Flux (neutron/cm²) at 40K feet (normal cruising altitude: 30-37K feet)
Aerospace Radiation Characteristics

**FIT rate at sea level**

- FFs (10Kb to 1Mb) : 1 to 2 FIT/Mb
- LUTMs (200Kb to 10Mb used from configuration memory)
- BRAMs (1Mb to 40Mb) : 60 (28nm) to 800 (130nm) FIT/Mb
  - (50 to 200 FIT/Mb from alpha particles)
- Config Mems (5Mb to 200Mb) : 70 (28nm) to 450 (130nm) FIT/Mb
  - (30 to 150 FIT/Mb from alpha particles)

**FIT rate at 40K feet over equator / poles**

Deterioration by a factor of over 100x/560x (as compared to sea level)

FIT = Failure In Time

May, 2012
Aerospace Radiation Characteristics

<table>
<thead>
<tr>
<th>Technology Node</th>
<th>Product Family</th>
<th>Neutron Cross-section per Bit (1)</th>
<th>FIT/Mb (Alpha Particle) (2)</th>
<th>FIT/Mb (Real Time Soft Error Rate) (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Configuration Memory</td>
<td>Block Ram</td>
<td>Error</td>
</tr>
<tr>
<td>250 nm</td>
<td>Virtex</td>
<td>9.90 x 10^{-15}</td>
<td>9.90 x 10^{-15}</td>
<td>±10%</td>
</tr>
<tr>
<td>180 nm</td>
<td>Virtex-E</td>
<td>1.12 x 10^{-14}</td>
<td>1.12 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>150 nm</td>
<td>Virtex-II</td>
<td>2.56 x 10^{-14}</td>
<td>2.64 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>130 nm</td>
<td>Virtex-II Pro</td>
<td>2.74 x 10^{-14}</td>
<td>3.91 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>90 nm</td>
<td>Virtex-4</td>
<td>1.55 x 10^{-14}</td>
<td>2.74 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>65 nm</td>
<td>Virtex-5</td>
<td>6.70 x 10^{-15}</td>
<td>3.96 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>40 nm</td>
<td>Virtex-6</td>
<td>1.26 x 10^{-14}</td>
<td>1.14 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>90 nm</td>
<td>Spartan-3</td>
<td>2.40 x 10^{-14}</td>
<td>3.48 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>90 nm</td>
<td>Spartan-3E</td>
<td>1.31 x 10^{-14}</td>
<td>2.73 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>45 nm</td>
<td>Spartan-6</td>
<td>1.00 x 10^{-14}</td>
<td>2.20 x 10^{-14}</td>
<td>±10%</td>
</tr>
<tr>
<td>28 nm</td>
<td>7 Series FPGAs</td>
<td>6.99 x 10^{-15}</td>
<td>6.32 x 10^{-15}</td>
<td>±10%</td>
</tr>
</tbody>
</table>

Notes:
1. Data from Los Alamos Neutron Science Center (LANSCE).
2. Spartan-6 and 7 series FPGAs data based on thorium foil testing and package alpha emissivity of 0.0015 counts/cm²/hr. Virtex-6 FPGA alpha data estimated using Virtex-6 Real Time Soft Error Rate Results.
4. 90% confidence interval.

May, 2012
4. SEE Mitigation Techniques

Which are the strategies to mitigate SEE’s?

- Technological
  - Design
  - Software and Hardware Redundancy

COTS – cost-effective

Space / time

- Fault detection (on-chip monitoring)
- Error correction
- Observe, adjust along product lifetime
Key areas in the FPGA tissue

- Configuration memory
- Functional:
  - BRAMs
  - LUTs
  - FFs
  - Lines

(set)
Soft Error Mitigation

MODULAR REDUNDANCY

DMR
TMR

Soft error

- SET (Single Event Transient)
- SEU (Single Event Upset)
- SEFI (Single Event Functional Interrupt)

Recoverable Errors

- SBU (Single Bit Upset)
- MBU (Multiple Bit Upset)

ECC (memory)

Scrubbing (configuration Memory)

SW redundancy (for processors)

May, 2012
Modular Redundancy: DMR / TMR

**Spatial DMR/TMR (Dual / Triple)**

**Advantages**
- Small or no time/performance overhead
- Specialized design tools available

**Disadvantages:**
- Over 2x(DMR)/3x(TMR) area overhead
- Over 2x/3x power consumption
- Unspecialized/generic design tools may undermine implementation (Excellent knowledge on design tool needed)

**Time DMR/TMR and SW redundancy**

**Advantages**
- Small(DMR/TMR)/no(SW) area overhead

**Disadvantages:**
- Over 2x(DMR)/3x(TMR) latency overhead
- Over 2x/3x power usage
ECC (Error Correcting Codes)

For memory, ECC technique is very efficient. Using, e.g., Hamming code, only 7/8b is needed to detect 2b errors and correct 1b error for each 32/64b. Of course, wider words will increase the code efficiency but will also increase the probability and the number of errors within each word. Both Altera and Xilinx have support for ECC implementation. There are some area and performance degradation, but much less than DMR.
ECC (Error Correcting Codes)

- BRAM hardware ECC support
- External RAM has SW IP core ECC support

Features specific to Virtex-6 FPGAs are shown in gray.
SEU in configuration memory is the main SEE concern for SRAM base FPGA technology. It can only be corrected by means of scrubbing/reconfiguration.

From ISE12 and on, with Virtex5 and later, Xilinx has free soft IP support for configuration scrubbing (SEM IP). It can detect and/or correct configuration memory errors. Also, it can, on demand, inject faults into the configuration memory for test and verification.

Furthermore, with more advanced version of this core and FPGA, it can detect if a SEU will affect or not the design functionality, allowing differentiated actions to be taken, so to improve system availability. As typically, only 10% of the entire configuration memory is essential for a given design functionality.

This has a small footprint and can be completely separated from the rest of the design. It takes several ms to complete 1 test cycle and depending on options, it may require additional external EPROM space.
Xilinx SEM IP

- **User interface for error injection**
- **Internal interface to access configuration memory**
- **ROM interface for error classification and/or repair**
- **Serial interface for status and/or error injection**

May, 2012
Xilinx SEM IP (Essential Bits)

Essential Bits are typically <1/3 of the Device Configuration Bits, while Critical Bits are 10 to 20%.
Altera Quartus II software has support for configuration memory scrubbing for all Altera’s FPGAs.

From 130nm process down (Stratix III and forward), Altera’s FPGAs have hard CRC core for configuration scrubbing. Older versions can use soft IP for the purpose.

It guarantee detection of up to 3 bits errors (latest model can detect up to 5 bits errors, corresponding a coverage of 99,9999%). Latest versions can also inject 1b or 2 adjacent bits faults into a frame of configuration memory.

Additional soft IP and external ROM can be used to implement the Critical Configuration Soft Error Detection. This will differentiate errors into critical errors and non-critical errors and different actions can be taken, so to improve system availability. As even with a fully occupied design, only 10% of the entire configuration memory is essential for system functionality.

It takes several ms to complete 1 test cycle.
Scrubbing (Altera)

Stratix III FPGA

CRC Engine (Hard Logic)

Location Information

Sensitivity Processor (Soft Logic)

Memory Access Logic

Serial/Parallel Flash

CRC Error

Critical Error

Readback bitstream with expected CRC included

32-Bit Error Detection CRC Calculation, Error Search Engine, and Internal Scrubbing

Error Detection State Machine

Control Signals

Error Message Register

Syndrome Register

Error Injection Block

Fault Injection Register

JTAG Fault Injection Register

JTAG Update Register

User Update Register

JTAG Shift Register

User Shift Register

JTAG TDO

General Routing

Altera WP-01012

Altera stx5_51011

May, 2012
Typical Techniques

Parity
Single error detection (SED):
- Signal on parity mismatch
- Optimized for speed and performance

Scrubbing
FPGA configuration bits validation:
- Configuration bits read back by hardware engine
- Compare to know good value
- Signal on mismatch

ECC
Single error correction, double error detection (SECDED):
- Detect and correct single bit errors
- Detect double bit errors
- Signal on either error correction or detection
- Health signal while system still operational
5. Long-term Effects Monitoring

Delay Sensor insertion in critical locations

CME: Critical Memory Element
DCM: Digital Clock Manager
Long-term Effects Monitoring

Delay Sensor architecture

Si_reg
Si
SRL16
RST
CLK
CLD
Q
D
D
CLK
CLK_d
DCM
LOCKED
OUT_SC
AS_FF2
OUT_AS
AS_FF1
RST
DCM
EN
Programmable delayed clock

PWD
Variable clock phase

DCM Controller
6. Standard Compliance

- **Medical products and equipment**
  - IEC 62304
  - IEC 60601

- **Automotive**
  - ISO 26262
  - AUTOSAR
  - AEC
  - SAE

- **Aerospace**
  - DO-254 (Hardware) - **ED-80** in Europe
  - DO-178 (Software)
Certification for Avionics

DO-254 (hw) and DO-178 (sw)
DO-254 Standard (Aerospace)

Typical FPGA design flow for the DO-254 lifecycle

(DO-254=ED-80 in Europe)
IP Compliance with DO-254

- Certified?
- Custom or COTS?
- Simple or Complex?
- Usage/deployment history
Tool Compliance with DO-254

Tools used in the entire process must themselves comply with DO-254
7. Avenues of Research

• Long-term Variability Monitoring
  – Delay monitors (our sensors)
    • For PVT A monitoring
  – Use of SEM IP for configuration memory monitoring
  – BRAMs as radiation sensors?
    • Use of embedded 8-bit ECC in active BRAM resources and
    • Activate unallocated BRAM cells as sensors
  – TMR with $f_2 > f_1$ in one module with Aging Sensors?
8. References

- http://www.xilinx.com/support/
- V. Bexiga, et. al., “Performance Failure Prediction Using Built-In Delay Sensors in FPGAs”, Proc. on Field Programmable Logic and Applications (FPL), Chania, Greece, Sep. 5-7, 2011
- http://www.autosar.org/
- http://www.aecouncil.com/

May, 2012