The Benefits and Limitations of SRAM Based Field Programmable Gate Array Fault Injection

Melanie Berg
MEI Technologies- NASA/GSFC Radiation Effects and Analysis Group

To be presented by Melanie Berg at the Single Event Effects Symposium, April 20-22, 2009 in La Jolla, CA, and to be published on nepp and radhome web sites.

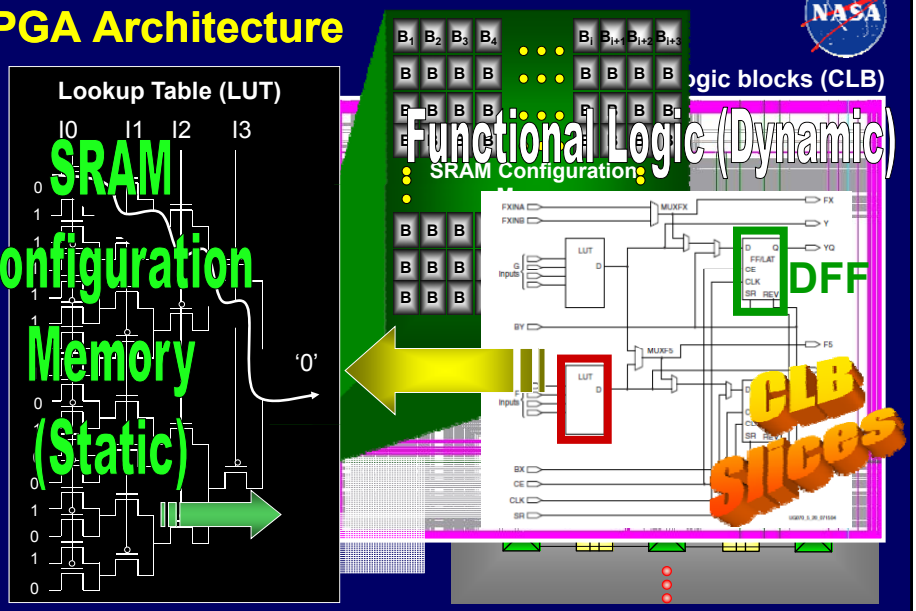
Motivation…Why Fault Injection (FI)?

- Part of the System Error Rate Prediction Process
- Enhances the device fault analysis process
  - Controlled error injection – no random components
    - Temporally
    - Physically
  - Specific Device mechanism and Error Signature analysis
    - Clock trees
    - Control structures
    - Routes
    - Logic
- Can reduce the amount of necessary beam time

Ability to hone in and analyze while saving money

To be presented by Melanie Berg at the Single Event Effects Symposium, April 20-22, 2009 in La Jolla, CA, and to be published on nepp and radhome web sites.

General Xilinx Virtex 4 SRAM-Based FPGA Architecture



To be presented by Melanie Berg at the Single Event Effects Symposium, April 20-22, 2009 in La Jolla, CA, and to be published on nepp and radhome web sites.

3

Xilinx SX55: Radiation Test Data

Xilinx Consortium: ***VIRTEX-4VQ STATIC SEU CHARACTERIZATION SUMMARY: April/2008***

Table 9c. CREME96 Calculated Orbital Upset Rates

Configuration Memory Cells
Upsets/Device-Day
Typical Solar Conditions

Orbit	LEO	LEO	POLAR	CONST.	GEO
Altitude (km)	400	800	833	1,200	36,000
Inclination	51.6°	22.0°	98.7°	65.0°	0°
XQR4VSX55	0.76	7.43	5.12	20.0	4.20

Table 9a. CREME96 Calculated Orbital Upset Rates

Functional Interrupts (All Virtex-4)
Upsets/Device-Day
Typical Solar Conditions

Orbit	LEO	LEO	POLAR	CONST.	GEO
Altitude (km)	400	800	833	1,200	36,000
Inclination	51.6°	22.0°	98.7°	65.0°	0°
POR	2.83E-06	2.73E-05	1.85E-05	7.36E-05	1.21E-05
SMAP FAR	2.25E-06	2.45E-05	1.69E-05	6.71E-05	9.46E-06
GSIG	1.57E-06	2.41E-05	1.57E-05	6.47E-05	4.87E-06

- Configuration SEU rate is significantly higher than all other components → focus is Configuration bit upset rates (not DFFs) and Single Event Functional Interrupts (SEFIs)

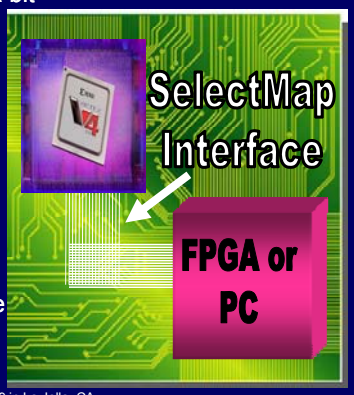
$$P(fs)_{error} \propto P_{Configuraton} + P_{SEFI}$$

To be presented by Melanie Berg at the Single Event Effects Symposium, April 20-22, 2009 in La Jolla, CA, and to be published on nepp and radhome web sites.

4

Basic Xilinx V4 FI Considerations

- **Where do we FI?… configuration memory**
- **How?**
  - Through Xilinx Parallel Configuration Interface (SelectMap)
  - Write to the Configuration Memory and flip a bit
- **What will get affected?**
  - Clocks
  - I/Os
  - Functional Logic
  - Routes
- **Temporal Dependencies?...**
  - While design is fully operational (Dynamic Testing)
  - STATE SPACE TRAVERSAL and Coverage
  - Error propagation to observation points



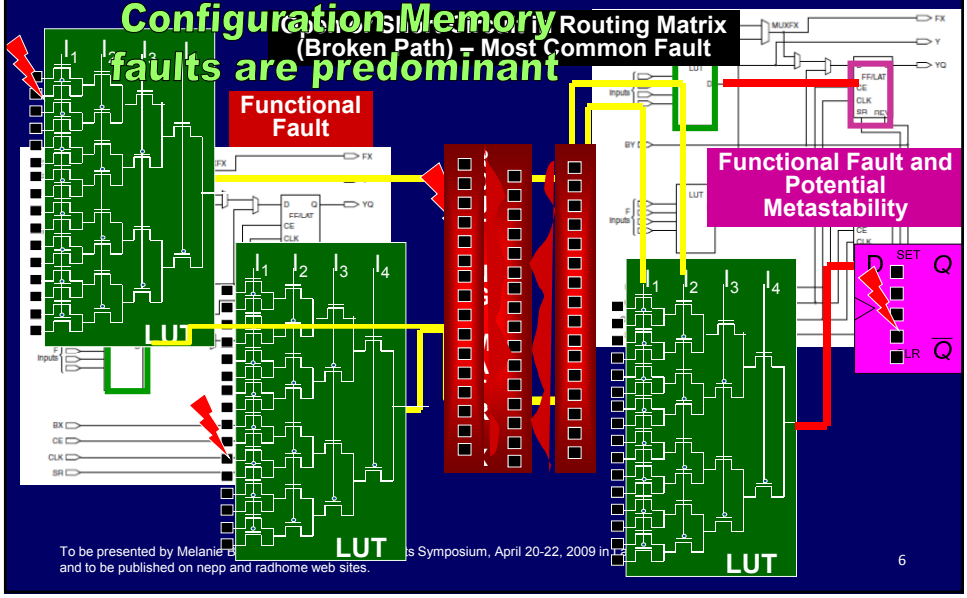
To be presented by Melanie Berg at the Single Event Effects Symposium, April 20-22, 2009 in La Jolla, CA, and to be published on nepp and radhome web sites.

5

Configuration Upset Effects

Without Mitigation

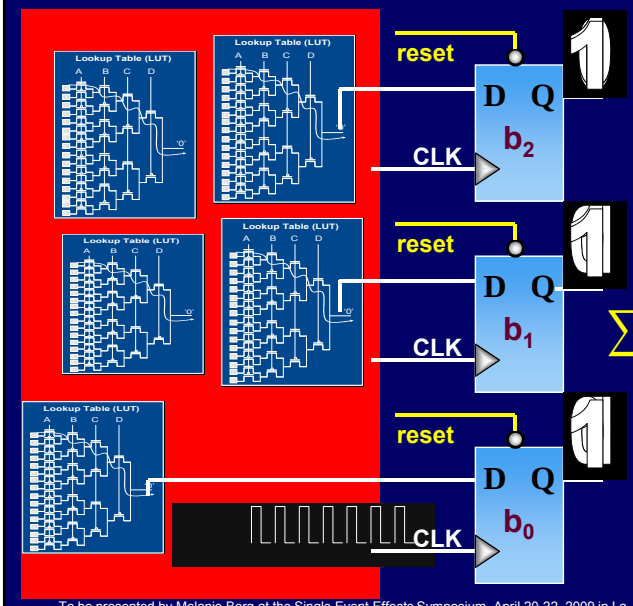
Configuration Memory faults are predominant



To be presented by Melanie B[illegible]s Symposium, April 20-22, 2009 in [illegible] and to be published on nepp and radhome web sites.

6

Design State Space $\sum = 2^{\#DFFs+INPUTS}$



$$\sigma_n = (b_0, b_1, b_3)$$

State$_n$ is defined by boolean values of inputs and DFFs

$$\sum = (\sigma_0, \sigma_1, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7)$$

State Transition $(\Re) \rightarrow$ Coverage:

- Coverage is defined by a set of State Transition Relations (R):
  - How many states have we transitioned from
  - How many states have we transitioned to
- Not all Transitions are valid within the state space Cartesian product
- Relations depend on current state, next state, and time

$$\Re \subseteq \sum \times \sum$$

$$\Re(\sigma_i, \sigma_k) \rightarrow true;$$

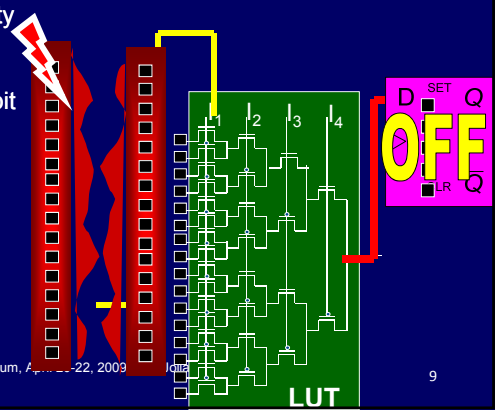
The relation holds true if and only if:

σ_i @ time t, and σ_k is a possible state @ time t+1

FI and Transitioning from State to State

- Transitioning to a state… will we ever get there?
  - Next cycle
  - Multiple cycles
  - Never
- FI & State Reachability
  - May never reach a state that faulty bit affects
  - Does faulty bit disrupt operation?
  - We have to run the test with the bit in fault long enough
    - Weeks or years
    - Unrealistic
  - We have to toggle all inputs
    - Time dependent
    - State dependent

DFF is off Because we haven't reached the state yet WILL NOT CATCH ERROR

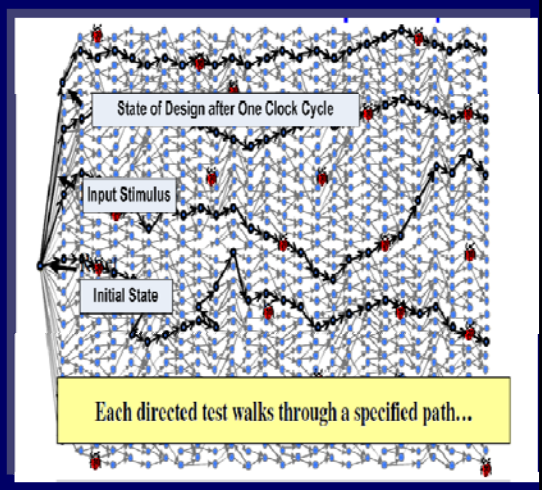


FI and Transitioning from State to State

- We have to run the test with the bit in fault long enough
  - Weeks or years
  - Unrealistic
- We have to toggle all inputs
  - Time dependent
  - State dependent
- Configuration Bits that have been flipped while their corresponding circuitry has been turned off can lead to a lower potential error calculation
  - Detrimental to Critical Space Projects
  - Need upper bounds not lower bounds

Examples of Reachable States that are Problematic to FI

- Detrimental Latency Circuits: Triggers
  - Count and fire (every n number of cycles…)
  - External Interrupt (non-deterministic)
- Exponential Explosion: Decoded Events
  - Can generally have many hardware decision branches
  - Time to get to a state

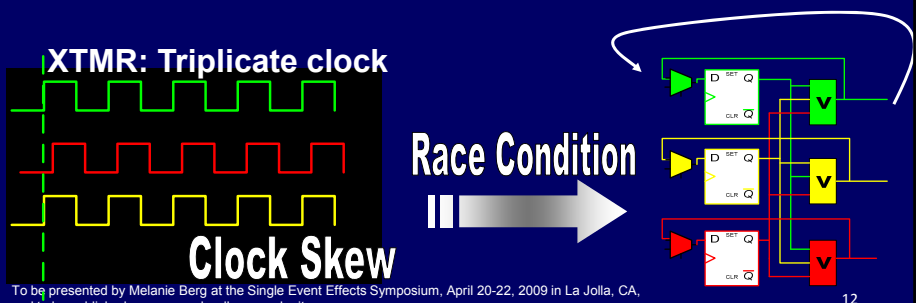


To be presented by Melanie Berg at the Single Event Effects Symposium, April 20-22, 2009 in La Jolla, CA, and to be published on nepp and radhome web sites.

11

Getting Back to Our Goal

- Want to determine how many bits out of the configuration memory can disrupt operation
- Why?
  - Fault prediction→ $\frac{dE}{dt} <= \#ConfigurationBits * \frac{dE_{configBit}}{dt}$
  - Mitigation Integrity Dynamic analysis



To be presented by Melanie Berg at the Single Event Effects Symposium, April 20-22, 2009 in La Jolla, CA, and to be published on nepp and radhome web sites.

12

What Has REAG Accomplished with FI

- Xilinx Design Tool Reports Resource Utilization (CLB specifics)… i.e. 99% LUT; 80%DFF
  - Not accurate enough to determine configuration bit percentage
    - CLB information accounts for 11% of the device
    - Many CLB bits are unused
- Most bits are routing – need fault injection to determine impact
- REAG is Investigating various designs… Can an upper limit be found?:
  - Simple routing structures 98% SLICE capacity: 1% of configuration bits can disrupt circuit
  - Complex routing structures 98% SLICE capacity: 15% of configuration bits can disrupt circuit

Analysis

- Should not use percentage device utilization for fault prediction – can obtain a gross overestimate and subsequently over design
- Complex designs may never attain higher than 30% of potential configuration bits that can cause fault
- Using Fault Injection on an actual complex circuit may not capture all potential failures
  - Investigation needs to be expanded to determine if saturation can be observed
  - Complex designs can then probably be bounded

Conclusion

- The goals of FI are:
  - To assist in fault prediction
  - Analyze design integrity
- FI in SRAM Based FPGAs can be preformed by flipping the state of configuration bits via the SelectMap Interface
- In order to determine if the bit can cause an error the design state space must be covered
- Complete State space coverage is generally impossible because:
  - Actual Complex Flight designs have an exponentially large state space and an exponentially large set of transitions
  - A considerable amount of the state space needs to be covered per fault
- REAG is currently investigating various designs to determine how to apply upper-bound estimates for configuration bit upset prediction
- REAG has successful illustrated the benefits of FI in design integrity dynamic testing