RobustScan™

Platform for Soft-Error Protection Using Robust Scan Cells

SYNTEST

The Testability Company

Soft errors, also referred to as **single-event upsets** (SEUs), are transient faults caused by various types of radiation. Radiation-induced transient faults can abruptly flip the stored state of a system and cause a system crash or even worse - a **silent data corruption** (SDC) - if they are undetected.

Atmospheric radiation, such as cosmic rays, have long been regarded as the major source of soft errors, especially in memories, and chips used in space applications typically use parity or error-correcting code (ECC) for soft-error protection. As process geometries continue to scale down, the amount of energy required to cause an error is lowered. Reduced feature sizes, higher logic densities, shrinking node capacitances, lower supply voltage, and shorter pipeline depth have significantly increased the susceptibility of integrated circuits (ICs) to SEUs. Terrestrial radiation, such as **alpha particles** from the packaging materials of the chip, is also starting to cause soft errors with increasing frequency. This has also created system reliability concerns, especially for chips used in the automotive, medical, and networking industries.

The **soft-error rate** (SER) of a system is generally measured in units of **Failures in Time** (FIT). A soft-error rate of 1 FIT means that the mean time before an error occurs is a billion device hours. A SER of 114 FITs, which a large US integrated device manufacturer (IDM) targets for undetected errors caused by SEUs, would require roughly 1,000 years for an SEU to cause an undetected error.

Recent study reveals that for an IC designed with feature size smaller than 65 nm, all memories, combinational logic, and sequential elements (such as scan cells) are more susceptible to soft errors. Since parity or ECC circuits are often used to protect memories from soft errors, the remaining issues are how to identify and harden or protect those scan cells and combinational logic that are also susceptible to soft errors.

A traditional approach is performing SER analysis on the entire design at the gate level to spot the logic blocks that are most susceptible to soft errors. The quantitative FIT metric is used to measure SERs before and after selection of these most-susceptible cells (scan cells and combinational cells). SER analysis can be performed iteratively to trade-off the best resulting **robust design** to also meet customer expectations on additional area, timing, and power considerations.

Benefits of RobustScan™

- Reduces soft-error rate (SER) of a system by 20X to 1,000X
- Increases system reliability through online soft-error protection
- Performs SER analysis to identify logic blocks (e.g. combinational cells and scan cells) that are most susceptible to soft errors
- Automatically replaces selected scan cells with robust scan cells that can detect or correct the soft errors, given an SER reduction requirement.
- Automatically replaces selected combinational cells with hardened combinational cells that can reduce the SERs of these selected combinational cells and overall SER of the chip
- Supports existing circuit-level soft-error protection logic (referred to as robust scan cells) currently practiced in industry or proposed in academia
- Accepts user-defined robust scan cells and hardened combinational cells
- Short development time, no iterations
- Integration w/ scan synthesis/ ATPG
- Predictable & low hardware overhead
- Debug/diagnosis features

Features of RobustScan™

- User-selectable patented configurable soft-error resilience (CSER) cells or user-preferred SER mitigation cells
- SER analysis, robust-scan-cell and hardened-combinational-cell selection and synthesis, and testbench generation
- Third-party scan synthesis, SER analysis tool interface
- SynTest DFT/diagnosis tool interface

To protect a scan cell, the scan cell can embed an error-detection or error-correction circuit for soft-error protection. It is also possible to harden the scan cell by sizing up the latches. The resulting scan cell is referred to as a **robust scan cell**. Combinational logic is less susceptible to glitches than unprotected memories. First, the glitch must be of sufficient strength to propagate from the location of the strike, through each stage of the combinational logic, until it reaches an output; otherwise, the glitch is attenuated and the transient error is **electrically masked**. Second, the glitch needs to have a functionally sensitized path to a latch; otherwise, the glitch is **logically masked**. Finally, the timing of the glitch must be such that the glitch arrives at a latch during its latching window; otherwise, the glitch is **latching-window masked**. However, a study on the susceptibility of combinational logic to soft errors has found that combinational logic is becoming a growing concern on reliability, even if these masking factors exist.

Thus, to cope with soft errors, one must incorporate effective protection mechanisms for combinational logic and scan cells, in addition to memories. The RobustScan™ platform allows users to synthesize soft-error protection logic for such selected cells and generate needed testbenches to verify the correctness of the synthesized robust design.

The RobustScan™ Platform

The RobustScan™ platform consists of four major tools:

- **Soft-Error Rate (SER) Analysis** – allows users to identify and report the most susceptible logic blocks and run trade-offs to determine the best soft-error mitigation technique at the gate level.
- **Robust-Scan-Cell and Hardened-Combinational-Cell Selection** – allows automatically selecting or accepting a set of scan cells and combinational cells for soft-error protection, based on customer expectations on SER reduction.
- **Robust-Scan-Cell and Hardened-Combinational-Cell Synthesis** – allows automatically replacing the set of selected cells with user-defined robust scan cells and hardened combinational cells, and stitching them into an existing scan design.
- **Testbench Generation and Verification** – automatically generates Verilog testbenches to verify the correctness of the robust design.

The inputs to the SER analysis program include a scan-inserted netlist, SDF file, library cells, and input constraints related to radiation flux. The program can also optionally accept a pre-selected list of robust scan cells and hardened combinational cells. After SER analysis, the program will report the SER of the overall design and identify the logic blocks (signals of scan cells and combinational cells) that are most susceptible to soft errors.

Based on the analysis results, the robust scan selection and synthesis programs will automatically select signals from the SER analysis program or accept a new user-supplied signal name list, then replace each selected cell with a user-defined corresponding robust scan cell or hardened combinational cell. The inserted and stitched design is a robust design.

Finally, the testbench generation program will create additional Verilog testbenches to verify whether the robust design will operate correctly in all modes defined in the robust scan cells.

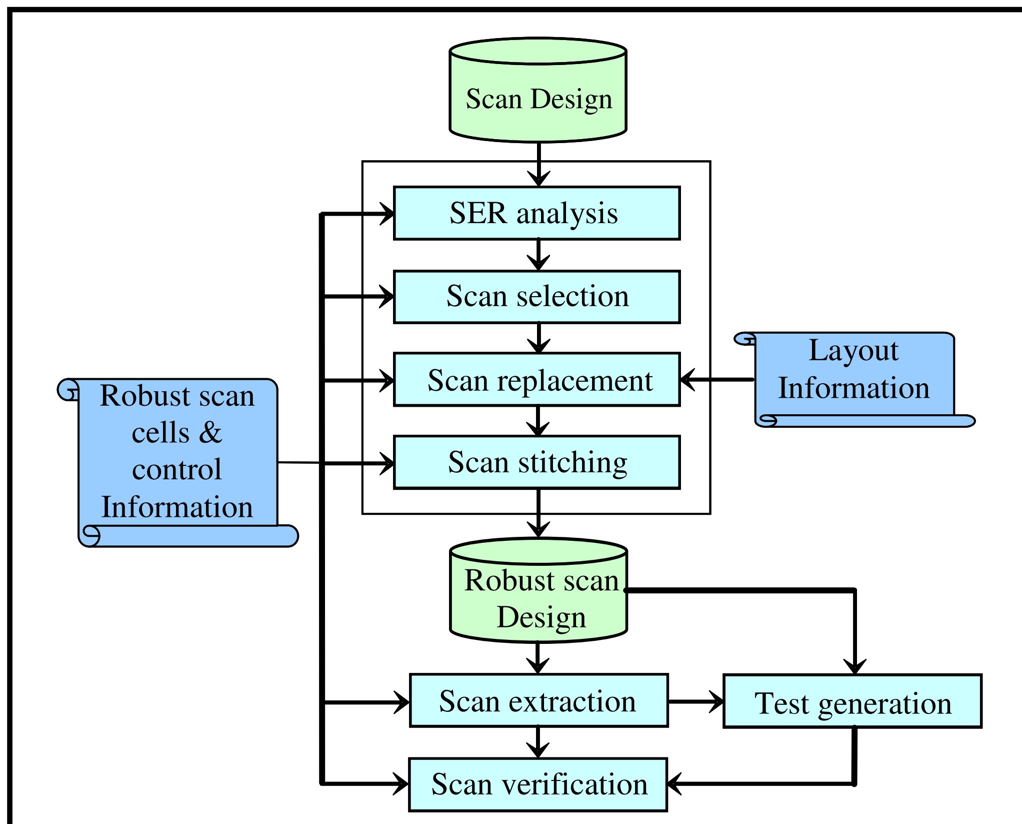
CSER – Configurable Soft-Error Resilience Cell

RobustScan™ currently supports a few robust scan cells, called **configurable soft-error resilience (CSER)** cells. The CSER cell can be also user-defined or a SER mitigation cell practiced in industry, as permitted for use by the user company.

PATENTS

SynTest products are protected by one or more of the patents listed in http://syntest.com/patent.htm.

Patents pending in the U.S. and other countries.



SynTest Technologies, Inc.
505 S. Pastoria Ave, Suite 101, Sunnyvale, CA 94086
Tel: 408-720-9956   Fax: 408-720-9960

www.syntest.com
info@syntest.com

© 2014 SynTest Technologies, Inc. All trademarks and registered trademarks are the properties of their respective owners.