Contribution ID: **105** Type: **Poster**

SEU injection framework for radiation-tolerant ASICs, a formal verification approach

Thursday 22 September 2022 16:40 (20 minutes)

Single Event Upsets (SEUs) represent a major challenge for digital electronics operated in a radiation environment.
Triple Modular Redundancy (TMR) is one of the most popular approaches to increase digital electronics resilience to SEUs.
Simulation is the most used approach for verifying the correct triplication of the designs.
This contribution describes a novel approach for verifying the triplication.
A formal verification tool is used, removing the need for a complete functional verification framework for the SEU injections in the design.
The approach allows finding bugs earlier in the design phase hence reducing the development and debug time.

Summary (500 words)

The high flux of ionising particles in the CERN experiments' detectors poses a challenge to the design of digital electronics as they are responsible for Single Event Effects (SEEs).
A popular approach to limit the SEEs susceptibility consists in applying Triple Modular Redundancy (TMR) to the design.
The design triplication can be done with partially automated tools such as TMRG.

To verify that the triplicated design is resilient to SEEs, a popular approach is to run functional verification while randomly injecting SEEs into the design.
This task, however, requires to have both an advanced top-level netlist and a functional verification framework which are generally available only at a later stage of the project.
Moreover, the SEEs fault injection is a long and resource-intensive process which can go on for months.

Formal verification is a methodology, orthogonal to simulation, that allows mathematically proving given properties or providing counterexamples.
The obtained proofs are valid under the assumptions that are provided as input to the tool.
The approach presented in this contribution targets verifying the design susceptibility to Single Event Upsets (SEUs) using a formal verification methodology.
The only prerequisite for running the proof is to have access to the Design Under Test (DUT) synthesised netlist and it does not require to have a functional verification framework in place.
Moreover, the proof can be run on a module or partition of the design, without the need for having completed the design.
The identification of triplication issues in an early design phase allows for faster correction and low turn-around time.
In principle, the approach can work without any hypothesis about the design operation scenarios.

The methodology works as follows.
First, the list of the faultable nodes is extracted from the synthesises netlist.
Then a set of assertions and assumptions for each faultable node is generated, together with a startup condition that represents the state of the design after reset.
A fundamental part of this step is instrumenting the standard cell primitives to allow the formal tool to inject

SEUs into the sequential logic.
Finally, the formal proof is started.

This approach was used, so far in different designs: the slow-control logic of EXP28, a CERN 28 nm test chip (A), a data formatter for CMS HGCAL ECOND (B), and a monitor module for ECOND (C).
Design A, containing 957 sequential elements (before triplication), achieved unbounded proof in 120 seconds.
Design B, containing 3968 sequential elements did not achieve a complete proof in 24 hours.
75 % of the assertions were proven, identifying multiple issues in the triplication of the module.
Design C, containing 6587 sequential elements, achieved unbounded proof in 500 seconds.

The limitations of the approach are that it can only inject SEUs and it currently only works with single-clock single-edge designs.
Even with these limitations, it allows greatly reducing the time dedicated to SEUs injection and the subsequent debugging.

Primary authors: PULLI, Adithya (CERN); LUPI, Matteo (CERN)

Presenter: LUPI, Matteo (CERN)

Session Classification: Thursday posters session

Track Classification: ASIC