

SEU and SET Mitigation Techniques for FPGA Circuit and Configuration Bit Storage Design

David G. Mavis and Paul H. Eaton
Mission Research Corporation
5001 Indian School Road NE
Albuquerque, NM 87110-3946

Cosmic-ray heavy ions have long been known to cause Single Event Upsets, or SEUs, in FPGA (Field Programmable Gate Array) data latches as well as configuration bit storage latches. In addition to these "conventional" SEUs, cosmic rays also induce transients in combinatorial logic, in global clock lines, and in global control lines. These single event transients, or SETs, had only minor effects in earlier 0.8 to 0.7 micron technologies since the speed of these circuits was insufficient to propagate the 100 to 200 ps wide SET any appreciable distance through the circuit. However, as smaller feature size (and thus faster) technologies find their way into spaceborne systems, these transients quickly become indistinguishable from normal circuit signals.

In our paper, we first clarify the impact that shrinking device sizes have had on SEUs in spaceborne microelectronics due to the cosmic ray environment and explain how SETs in the combinatorial logic of a circuit have become increasingly important as spaceborne systems begin using FPGAs having device feature sizes smaller than 0.35 micron. We finally describe a circuit design methodology that can, with minor tradeoffs, totally eliminate SEUs, SET induced upsets, and even multiple bit upsets (MBUs) from FPGA circuit designs.

If a heavy ion strike occurs within the combinatorial logic block of a sequential circuit, and the logic is fast enough to propagate the induced transient, then the SET will eventually appear at the input of a data latch where it may be interpreted as a valid signal. Similar invalid transient data might appear at the outputs of lookup tables (LUTs) and on routing lines due to SETs generated in the programming elements, particularly for the case of EEPROM storage elements. Whether or not the resulting SET gets stored as real data depends on the temporal relationship between its arrival time and the falling edge of the clock. Similarly, SETs on clock, reset, and control lines can result in the storage of incorrect data within the data latches.

While conventional SEU error rates are independent of the chip clock frequency, SET induced error rates increase in direct proportion to the operating frequency. This error rate relation actually compounds the SET problem as technology feature sizes shrink since smaller feature sizes result in smaller gate delays that permit circuits to be operated at higher clock frequencies. Not only does each combinatorial gate in the circuit contribute to the SET error rate (because transients are no longer attenuated), but the probability of storing any given transient error will also increase (because of the higher clock frequencies). Shrinking device sizes have had serious, if not grave, implications for FPGA devices used in cosmic-ray environments. We demonstrate that, for typical FPGA designs, SET induced error rates may actually exceed the SEU rates of unhardened latches as clock speeds approach 100 MHz for CMOS designs.

Nonvolatile, reprogrammable FPGAs typically use EEPROM transistors to store the configuration data. We describe how SET pulse broadening occurs in devices that use EEPROM

transistors in an active fashion. The programmed threshold voltage of a EEPROM transistor is simply not large enough to provide charge dissipation drives comparable to normal CMOS transistors. This results in relatively wide SETs that are shown to propagate in FPGAs fabricated in technologies having feature sizes as large as 0.8 micron. The SET induced error rates in these cases can actually exceed SEU rates at frequencies of only a few tens of MHz.

We describe a new latch design that gives any sequential integrated circuit total immunity to both single event upsets and to single event transients. Sequential circuitry has combinatorial logic that outputs data and latches that sample and hold the data. According to the design, a temporally and spatially redundant latch is immune to (1) upsets that might occur in the latch itself, (2) transients that might occur in the combinatorial logic, and (3) transients that might occur the clocking and control signals of the circuit. The new latch, termed the temporally redundant sampling latch, is intended to replace conventional latches in any sequential circuit, not just FPGAs, to provide high, or event total, immunity to heavy-ion induced upsets.

The temporally redundant latch achieves upset immunity as a consequence of two distinct parallelisms: (1) a spatial parallelism resulting from multiple parallel sampling circuits, and (2) a temporal parallelism resulting from a unique clocking scheme involving multiple time-spaced clock signals. Spatial parallelism prevents the usual SEUs in the static latches. Temporal parallelism provides upset immunity to SETs in combinatorial logic and global clock lines. It should be noted that SEU immunity is achieved solely through circuit function and not by any inherent immunity designed into the latches themselves through process or layout modifications.

Size and speed tradeoffs for the new design are minimal, considering that total SEU immunity can be achieved. Area penalties for typical FPGA designs will likely not exceed 10%. While simple clocking schemes incur a factor of two speed loss, more complex clocking can reduce the speed loss to a few percent.

Some FPGA vendors allow the user to program in triple module redundancy in an attempt to help mitigate conventional SEUs. This approach often neglects to consider SET effects, particularly in clock and control lines. For large redundant blocks of logic, with internal latches, error latency becomes an issue because it may be many clock cycles before an error gets flushed and the redundant blocks achieve resynchronization. In our temporal latch approach, the combinatorial logic is effectively replicated, not in space but in time. The same logic is really just used at three different times. The result of this, as described in the paper, is that errors are flushed on each clock cycle and the maximum error latency never exceeds a clock period.

Heavy-ion testing has, in the past, focussed primarily on detecting and characterizing conventional single event upsets in static latches. Special considerations must be observed to adequately detect and characterize SET induced errors, particularly in the presence of conventional SEUs. Chip clock speeds must be high enough to see SET induced errors over the conventional SEU background. Since test equipment may not function at adequate clock speeds, FPGA test approaches are discussed for which simple test circuits along with on-chip SET error detection is programmed into the device.