A Delay-efficient Radiation-hard Digital Design Approach Using CWSP Elements

Charu Nagpal Rajesh Garg Sunil P Khatri
Department of EE, Texas A&M University, College Station TX 77843.

Abstract

In this paper, we present a radiation-hardened digital design approach. This approach is based on the use of Code Word State Preserving (CWSP) elements at each flip-flop of the design, and leaving the rest of the design unaltered. The CWSP element provides 100% SET protection for glitch widths up to min$\{D_{min}/2, (D_{max}-\Delta)/2\}$, where D_{min} and D_{max} are the minimum and maximum circuit delay respectively and Δ is an extra delay associated with our SET protection circuit. The CWSP circuit has two inputs - the latch output signal and the same signal delayed by a quantity δ. In case an SET error is detected, then the current computation is repeated, using the correct output, which is generated later in the same clock period by the CWSP element. Unlike previous approaches, we use the CWSP element in a secondary path and the CWSP logic is designed to minimally impact the critical delay path of the design. The delay penalty of our approach (averaged over several designs) is less than 1%. Thus our technique is applicable for high-speed designs, where the additional delay associated with SET protection must be kept at a minimum.

1 Introduction

In recent times, there has been an increased interest in the radiation immunity of electronic circuits [1, 2, 3, 4, 5, 6]. This has been an area of significant interest and research for space or military electronics [5, 4, 7] for many years, due to the significantly larger rate of radiation strikes in such applications. For space applications, neutrons, protons and heavy cosmic ions which are trapped in geomagnetic belts produce intense showers of such radiation. When such ions strike diffusion regions in VLSI designs, they can deposit a charge, resulting in a voltage spike on the affected circuit node. If the magnitude of this spike is sufficiently large, an erroneous value may be computed by the circuit. This is particularly problematic for memories, since the stored state can flip as a result of such a radiation strike. Combinational logic may also be affected by such strikes, if the resulting glitch occurs at the time the circuit outputs are being sampled. Such bit reversals are referred to as Single Event Transients (SETs).

With the relentless shrinking of the minimum feature size of VLSI Integrated Circuits (ICs), there is a corresponding reduction in the dimensions of diffusion nodes. This results in a reduced diffusion capacitance, and hence, if charge is dumped on the diffusion node as a consequence of a radiation strike, a large voltage spike may be generated. With operating voltages getting smaller, this problem is further aggravated. As a result, modern VLSI ICs are significantly more prone to SET problems. Even though it is true that the amount of radiation received on the surface of the earth is lower than that in space, the shrinking of process feature sizes makes modern VLSI ICs more susceptible to SET problems than in the past [6].

The charge deposition rate is also referred to as the Linear Energy Transfer (LET). Cosmic ions have varying LETs, and they result in the deposition of a charge Q in a semiconductor diffusion region of depth t by the following formula [7].

$$Q = 0.01036 \cdot L \cdot t$$

Here L is the LET of the ion (expressed in MeV/cm^2/mg), t is the depth of the collection volume (expressed in microns), and Q is charge in pC. The amount of charge that is required to cause a bit to be sampled incorrectly is referred to as the critical charge, Q_C [8]. With diminishing process feature sizes and supply voltages, SET problems are a concern even for terrestrial electronics today, particularly for mission critical applications. Atmospheric neutrons as well as alpha particles which are created by unstable isotopes in the IC packaging materials can also cause SET problems. For reference, the LET of a 5 MeV alpha particle is 1 MeV/cm^2/mg [2]. Also, the probability distribution of energetic particles drops off rapidly with increasing LETs [9]. The largest population of particles have an LET of 20 MeV/cm^2/mg or less, and particles with an LET greater than 30 MeV/cm^2/mg are exceedingly rare [9, 10].

The current pulse that results from a particle strike is traditionally expressed as a double exponential function [11, 12]. The expression for this pulse is

$$I(t) = \frac{Q}{(\tau_\alpha - \tau_\beta)}(e^{-t/\tau_\alpha} - e^{-t/\tau_\beta}) \quad (1)$$

Here Q is the amount of charge deposited as a result of the ion strike, while τ_α is the charge collection time constant for the junction and τ_β is the ion track establishment constant. Based on the values used in [13], for the simulations reported in this paper, we used τ_β = 50ps and τ_α = 200ps. Also, since the results in [13] are reported for Q = 100fC and 150fC (based on [14]), we compare our results with those of [13] for the same conditions. Additionally, we provide results for other values of Q as well.

This paper uses the CWSP circuit of [15] to achieve SET tolerance. We refer to the normal circuit computation path as the *functional* path, while the alternative path used to detect and correct SET errors is called the *secondary* circuit path. The detection of a faulty computation (due to an SET event) is done on the secondary path by a watchdog circuit, which used CWSP elements. In case of an SET event, the correct value (which is computed by the CWSP element) is used to repeat the computation, after appropriately introducing a bubble in the computation pipeline. The main contributions of this paper are:

- We achieve SET tolerance for glitches of duration up to $min\{D_{min}/2, (D_{max}-\Delta)/2\}$, where D_{min}, D_{max} are the minimum and maximum delays of the design and Δ is an additional delay in the secondary circuit path. Since the CWSP elements are connected on a secondary as opposed to the functional computation path in the circuit, there is a minimal (less than 1% on average) speed penalty. This is achieved since the secondary circuit path containing the watchdog circuit is connected to the flip-flop inputs and outputs of the functional circuit in a manner that additional parasitic capacitances are minimized.
- Our results are better than those of [15], which has a delay overhead of 28.65%. Contrasted with an approach that employs gate resizing [13], our average circuit areas are comparable, while our delay penalties (0.54%) are much smaller than those of [13] (which has a delay penalty of about 2.8%).
- Our approach achieves 100% SET protection, which is not the case for [13], which guarantees 90% circuit protection.

The remainder of this paper is organized as follows: Section 2 discusses some previous work in this area. In Section 3 we describe our radiation hardened design approach for digital electronics. In Section 4 we present experimental results, while conclusions and future work are discussed in Section 5.

2 Previous Work

There has been a great deal of work on radiation hardened circuit design approaches. An excellent survey paper on this area is [16]. Several papers report on experimental studies in the area of logic circuits [7, 8, 17, 18, 5], while others have focused on memory design [19, 8, 6, 20, 3, 4]. Since memories are particularly susceptible to SET events, these efforts were crucial to space and military applications. Yet other approaches perform modeling and simulation of radiation events [12, 9, 2]. In [1], the authors address the sizing of transistors in a digital design in order to improve the radiation hardness of the design. In [6], the authors provide a built-in current sensor (BICS) to detect SET events in an SRAM. A radiation hardened DRAM design was proposed in [20], while a FLASH memory based FPGA was introduced in [5].

Other radiation hard design approaches tackle the problem of correcting errors at the system level, by using techniques such as triple modulo redundancy. A recent approach reported the use of Code Word State Preserving (CWSP) elements [21, 15] to achieve SET protection. This paper achieves the protection achieved by TMR [16], while using only two versions of any flip-flop/latch input signal (a regular version, and an appropriately delayed copy). In this paper, the CWSP element was introduced in the critical (functional) circuit path. This approach incurs a 28.65% delay penalty and a 17.6% area penalty (averaged over several designs) for

978-3-9810801-3-1/DATE08 © 2008 EDAA

tolerating a glitch of width up to 0.45ns. In contrast to [15], our CWSP elements are connected in a secondary circuit (i.e. *not* on the functional circuit path, thereby resulting in a minimal speed penalty (of less than 1%). Also, we have designed our circuits to tolerate SET glitches of widths up to 0.5ns and 0.6ns corresponding to Q = 100fC and 150fC (based on [14]). However, the circuit can easily be tuned to tolerate glitch widths of different magnitudes (up to $min\{D_{min}/2, (D_{max}-\Delta)/2\}$). This is discussed in further detail in Section 4.

Other approaches [22, 13] take the path of gate resizing for SET protection. Although this is orthogonal to our approach, we compare our results with [13] as well. We find that our average circuit areas are comparable with those of [13], and our delay penalties are 0.54%, versus about 2.8% for [13]. Also, our approach gives 100% SET protection compared to 90% coverage provided by [13].

Another class of approaches [23] is based on performing multiple strobing of the output data, with different delays between the strobes. With an odd (n $\geq$ 3) number of strobes, this approach achieves TMR, although along the time dimension. The multi-strobe TMR approach can tolerate glitch widths up to $D_{min}/2$. This is because the largest tolerable glitch width is half the interval between the first and last strobe. Since this interval is constrained to be less than or equal to D_{min} (the shortest circuit delay path), a multi-strobe TMR approach achieves a maximum SET glitch tolerance of $D_{min}/2$. However, for tolerating a glitch of width δ, this approach introduces an extra delay of 2δ plus the delay of the voting logic used to select the correct output value from the multiple strobed values. Note that this delay is in the functional circuit path. In contrast to this technique, our approach has a minimal delay overhead, since the computations which achieve SET hardening are done in a secondary path. A thorough comparison with [23] is not possible since no experimental results were provided in [23].

Other orthogonal approaches include [24], where SET protection is achieved by selectively shadowing the outputs of SET-susceptible gates, and connecting the original and the shadow gate by a pair of diodes. Although this approach also achieves 100% SET protection, it differs from ours in that it does not explore the time dimension in achieving SET protection.

3 Our Approach

Radiation strikes cause charge to be dumped on a diffusion node, which results in voltage glitches on these nodes. We are concerned with those glitches that cause nodes to change their logical value (i.e. those that cross the switch-point of the gate in question), and can be captured in a latch or flip-flop, thereby leading to incorrect circuit operation.

Our approach uses CWSP elements [15] to achieve 100% SET tolerance. In case of a SET event, the correct value is always computed by the CWSP element (which is connected in a secondary path, off the functional circuit critical paths). This correct value is used to repeat the computation in case of a SET event, by introducing a bubble in the computation. We achieve SET tolerance for glitches of duration up to $min\{D_{min}/2, (D_{max}-\Delta)/2\}$, without the added design cost associated with altering the original design. The CWSP element is connected to the flip-flop inputs and outputs, in a manner that the additional parasitic capacitances on the functional circuit path are minimized.

This section is divided into four subsections. In Section 3.1, we discuss, by way of introduction, the design of the CWSP element, and explain how it is utilized in [21, 15]. Section 3.2 explains our approach at the system level, while Section 3.3 provides details about the circuit level realization of our technique. A discussion on timing analysis is presented in Section 3.4

3.1 CWSP Element

We first discuss the structure of the Code Word State Preserving (CWSP) element, and how it is utilized in [21]. Figure 1 illustrates how CWSP elements are utilized in a circuit, using the approach of [21]. For the moment, let us assume that the CWSP element tolerates SET glitches of width up to δ, on any internal circuit node.

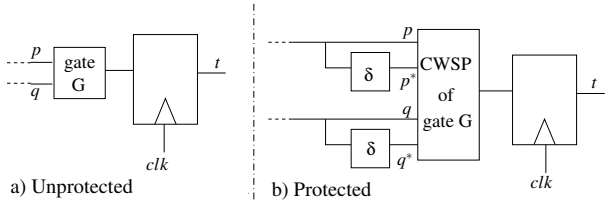


Figure 1: CWSP based SET Tolerance of [21]

Consider the gate in the original design as shown in Figure 1 (a). In the CWSP-based SET-resilient design approach of [21], each gate whose output is connected to a flip-flop input is replaced by a corresponding CWSP element, as shown in Figure 1 (b). For a k input gate, the CWSP element has $2k$ inputs. One set of k inputs are connected to the inputs of the gate that the CWSP element replaces. The other set of k inputs are connected to the delayed version (by a delay value δ) of the first set of k inputs. This is illustrated in Figure 1. The resulting circuit of Figure 1 (b) tolerates SET glitches of width up to δ.

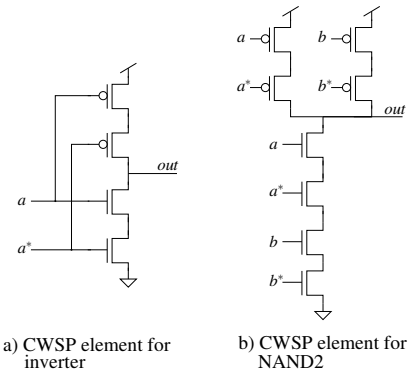


Figure 2: CWSP Elements for NAND2 and INVERTER Gates

We next explain how a CWSP element tolerates glitches of width up to δ. Figure 2 illustrates the CWSP circuits for an inverter and a NAND2 gate. In Figure 2, the inputs a and b are the un-delayed inputs, while the inputs a^* and b^* are delayed versions of a and b respectively (delayed by δ time units). Consider the CWSP element of either the INVERTER or the NAND2 gate. When the input $a = a^*$, and $b = b^*$, each CWSP element behaves normally, and the outputs are resistively driven to $\overline{a}$ and $\overline{a \cdot b}$ for the INVERTER and the NAND2 gate respectively. However, whenever there is an SET event which results in a glitch on any input, the gate stops driving the output resistively, since both the pullup and pulldown paths are disabled. At this point the output is held to its last correct value.

The problem with this approach is that the CWSP element which replaces a k-input NAND or NOR gate requires $2k$ series devices, making the approach impractical for gates with more than 2 inputs. This is because in bulk CMOS technologies, it is not practical to connect more than 4-5 series devices in series, due to body effect [25]. [15] improved upon the approach of [21] to resolve this issue. As shown in Figure 3, [15] uses only one type of CWSP element. In particular, this is the CWSP element of an inverter.

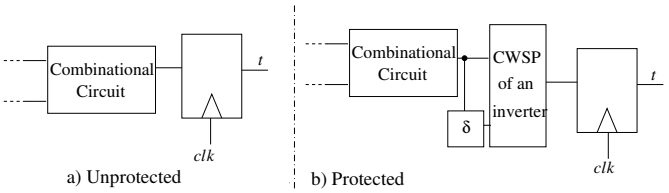


Figure 3: Improved approach of [15]

In this approach, one of the inputs to the CWSP element comes directly from the combinational circuit, while the other input is the same output, delayed by δ. The combinational circuit is implemented to generate the compliment of the required output, and the CWSP element provides another inversion. Since this element has at most 2 series devices, the delay and area overhead is kept at a minimum. This approach also averts the need to have a unique CWSP element for each library gate in the circuit, reducing the design time and cost. However, in both [15, 21], the delay of the circuit is increased significantly as CWSP elements are added before every flip-flop in the design. In particular, if an SET event results in a glitch of width δ at the un-delayed input to the CWSP element, it will attain its correct value after time δ. The delayed input attains its correct value after another δ delay. Thus, the output of the CWSP element is guaranteed to be correct after a delay of 2δ. This causes delay penalty of 2δ in the functional circuit delay. Additionally, the delay of the CWSP element (D_{CWSP}) is more than the delay of the gate it replaced (D_g), resulting in a further increase in the delay penalty. The delay overhead is therefore given by:

$$Delay = 2\delta + D_{CWSP} - D_g$$

In our approach, delay is only *minimally* increased since the computation of the correct value using the CWSP elements is done on a secondary path, unlike [15].

The work of [15] does not take into account a possible SET strike at the output of the CWSP element. In our approach, we have upsized the

CWSP element to ensure that it does not result in a SET glitch, for a strike with collected charge up to some value Q. The maximum value of Q used was 150fC. Note that this upsizing of the CWSP devices also helps ensure that the capacitances at its nodes are high enough that the CWSP element is able to hold its last correct state when there is an SET event resulting in a glitch on one of its inputs.

3.2 System Level Design

Figure 4 illustrates our approach schematically. Consider a fragment of the original design, shown in Figure 4 (a). This consists of a combinational output which is connected to a flip-flop labeled *DFF_system*. This flip-flop is in the functional circuit path of the design.

Our CWSP based modification to this circuit is shown in Figure 4 (b). The original combinational logic is left intact, except that the flip-flop is redesigned and renamed $DFF\_modified$ (this design is discussed later). In addition, the values of the D and Q signals of the flip-flop are read by the SET protection logic shown in Figure 4 (b). This logic is on a secondary path, and hence the functional delay is impacted only minimally. The D input of $DFF\_modified$ is connected to a minimum-sized inverter, whose output is fed directly to a CWSP element. The other input of the CWSP element is the delayed version of the inverter output (delayed by δ). The output of the CWSP element (called CW) is compared with the Q output of the system flip-flop using a rising-edge triggered equivalence checking circuit, with an output EQ. As explained in Section 3.1, the output of the CWSP element is guaranteed to be correct after a delay equal to the sum of 2δ and the delay of the CWSP element. Thus, the equivalence check is triggered after the rising edge of CLK, delayed by the sum of 2δ and the delay of the CWSP element. This delayed clock signal is referred to as CLK_DEL. Under normal operation, we note that EQ is high, since Q is equal to CW. When there is an SET event, these values can be different causing EQ to fall. In this case, the current computation is redone using the output of the CWSP element (which is guaranteed to be correct) as the input to $DFF\_modified$ in the next clock cycle.

Note that if an SET event is detected at any flip-flop in a design, the computation needs to be redone for all the flip-flops in the design. Consider that a design has n flip-flops. Suppose $EQ1$ through EQn are the outputs of the Equivalence Checkers corresponding to each of these flip-flops. If any of these EQ signals becomes low, the computation needs to be redone for all the flip-flops. A logical AND of all the EQ signals is therefore computed to obtain a global EQ signal (called $EQGLB$). If the signal $EQGLB$ falls, the value of CW is latched into a flip-flop (DFF2), whose output is CW^*. This value is guaranteed to be error-free[1], and is now used in the next cycle as the input to $DFF\_modified$, so that the current computation is redone in the next cycle.

We next explain the purpose of the flip-flop used to latch the value of $EQGLB$ to produce the signal $EQGLB_F$. Say there is an SET event in the clock cycle i which causes the output Q_i of the $DFF\_modified$ to be different from the input D_i. This will cause EQ, and thereby $EQGLB$ to fall. In the next $(i+1)^{th}$ clock cycle, CW^* (which is equal to D_i) will be latched to the system flip-flop $DFF\_modified$. However, CW is computed using D_{i+1}, which can be different from D_i. In the absence of the flip-flop which generated $EQGLB_F$, EQ and $EQGLB$ will remain low in the cycle $i+1$, again triggering a recomputation in the next cycle. This recomputation could go on indefinitely. The likelihood of two strikes on our SET tolerant design in two consecutive clock cycles is extremely low[2]. Hence, if there was an SET event in clock cycle i which resulted in EQ to be low, we can safely assume that there will be no SET event in clock cycle $i+1$. As a result, the EQ and $EQGLB$ signals can be ignored in the $(i+1)^{th}$ cycle. This can be done by making EQ and $EQGLB$ high in the next clock cycle. To achieve this, the value of $EQGLB$ is latched to $EQGLB_F$ at the positive edge of CLK. Following an SET error in cycle i, a low value on $EQGLB$ leads to CW^* being used as the input to $DFF\_modified$ for cycle $i+1$. In the Equivalence Checker (Figure 5), in cycle $i+1$, $EQGLB_F$ being low will make EQ high and no recomputation will be triggered in cycle $i+2$. At the architectural level, the decision to reapply the primary inputs and trigger a recomputation is done if the value of $EQGLB$ is low at the rising edge of CLK. This ensures proper handling of glitches as explained below.

As long as the CWSP element is sized appropriately to sustain an SET event which results in a glitch of size δ (the derivation of δ will be described in Section 3.4), the circuit is able to correct 100% of the SET events. To validate this claim, we consider several cases listed below. *We have simulated each of the scenarios below to confirm that our approach indeed provides 100% SET tolerance.* Note that it is reasonable to assume that there will not be more than one SET event occurring simultaneously. Thus, all the nodes in our protection scheme are analyzed independent of the others.

- Suppose there is an SET event in the CWSP circuit, or on its inputs. In this case, the CWSP element protects against this glitch, as discussed.
- If there is an SET event in the transitive fan-in of P or P^*, then this would have caused the values of P and P^* to be different in the worst case, causing the CWSP element to protect against the glitch.
- If the glitch is caused on Q, then the set of flip-flops that are sequentially adjacent to $DFF\_modified$ are responsible for protecting against it. Since *all* flip-flops are implemented with CWSP elements, this causes no erroneous computations. Further, if a glitch on Q causes EQ to be driven low, then the current computation is redone (albeit needlessly). However, no incorrect computation is performed.
- If an SET event in the Equivalence Checker circuit or the AND gate $AND1$ causes EQ and thereby $EQGLB$ to become low, there are two scenarios to be considered.
  - If the glitch is present at the positive edge of CLK, it will lead to a recomputation. Since only one SET glitch can occur at a time, the value of CW^* will be correct, so the correct computation is redone (albeit needlessly).
  - A glitch on $EQGLB$ at any other time is neither latched to $EQGLB_F$ nor it is used to determine the input to $DFF\_modified$ for the next clock cycle. It is therefore silently ignored. Also, since the decision to trigger a bubble in the pipeline at the architectural level is made if $EQGLB$ is low at the positive edge of CLK, no recomputation will be triggered.
- If there is an SET event in DFF1, it may lead to $EQGLB_F$ being low. This will ensure that EQ becomes high in the next clock cycle, which is benign considering that the probability of two strikes in two consecutive clock cycles is extremely low, as discussed earlier.
- If there is an SET event in DFF2, it might result in a glitch at CW^*. However, in that case, EQ would be high, and input D of the system flip-flop would be used for the computation. Thus, the glitch at CW^* is inconsequential.
- If there is an SET event at the output of the CWSP element, protection is achieved by appropriate upsizing of the transistors in the CWSP element.

The key features of our technique is that it achieves 100% SET tolerance, unlike [22, 13]. The SET correction circuitry is connected on a secondary path (not on the functional path), and hence the delay penalty is extremely small (much smaller than [22, 13, 15]). The system model requires recomputations in case of an SET event. A thorough simulation and analysis of a single CWSP element assures SET tolerance for the entire design. The technique can tolerate SET glitches up to a width $min\{D_{min}/2, (D_{max}-\Delta)/2\}$, where Δ is a fixed delay associated with the SET protection circuitry. The expression for Δ is derived in Section 3.4.

3.3 Circuit Level Design

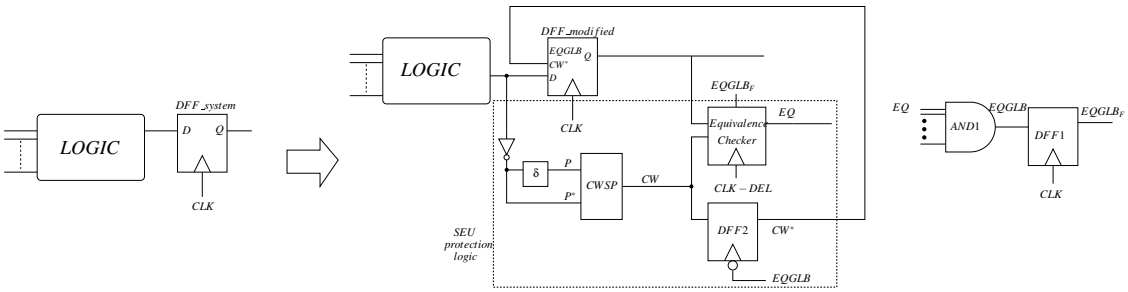
Figure 5 describes our technique at the gate level. The circuit blocks(*DFF_modified*, *Equivalence Checker* and $EQGLB_F$ *Circuit*) from Figure 4 are marked with a dotted outline in this figure. The CWSP element and its delay circuitry is not shown in Figure 5.

The *Equivalence Checker* block consists of a XNOR, followed by a MUX with $EQGLB_F$ as the select signal. The purpose of this MUX was explained in Section 3.2. The output of the MUX is fed to a flip-flop, which is clocked by the rising edge of CLK_DEL (CLK delayed by $2\delta + D_{CWSP}$). A logical AND of the EQ outputs of all the flip-flops in the design is used to generate the $EQGLB$ signal. Instead of using an AND gate, it is more area efficient to achieve the same functionality by performing a NOR of the inverted EQ signals. It was experimentally seen that the delay of the NOR gate with up to 30 inputs is reasonable (about 80ps). For designs with more than 30 flip-flops (EQ signals), a multilevel AND structure was used. Our experiments account for this. The Master latch of $DFF\_modified$ is modified so that when $EQGLB$ is high, the Master latch input is connected to D. When $EQGLB$ is low (in case of an equivalence check mismatch in one of the flip-flops), then the Master latch input is connected to CW^* (the guaranteed error-free value).

Devices in the SET protection circuitry are minimum-sized, to minimize the area overhead required to achieve SET protection. PMOS gate widths are made the same as NMOS gate widths, for the same reason. We simulated the entire circuit in SPICE, to verify for correct operation.

[1] if there is an error on CW^*, this error is silently ignored by the circuit

[2] As per [26, 27], the maximum solar proton fluence for particles of energy $>$ 1MeV based on the JPL- 1991 model is $2.91X10^{11}/cm^2/year$ with 99% confidence. The maximum area and time period for the testcases run was seen to be $473.4X10^{-8}cm^2$ and $5.5ns$ respectively. Using these values, we can show that the maximum number of particle strikes in the testcases run in two consecutive cycles is $4.78X10^{-10}$.



a) Original Circuit b) Modified Circuit c) $EQGLB_F$ Circuit

Figure 4: Architectural view of our SET Tolerant Design

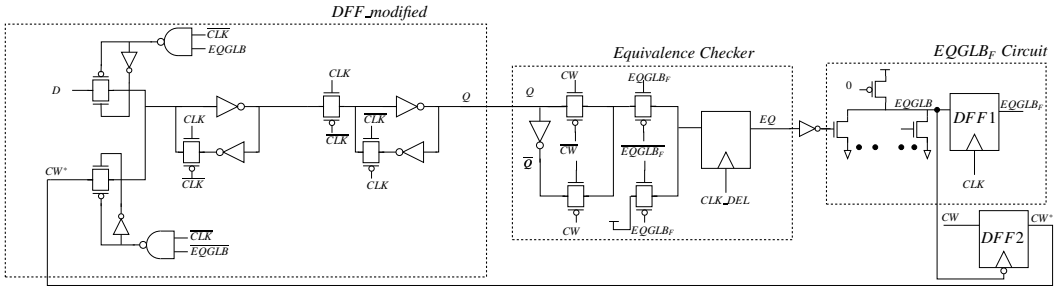


Figure 5: Gate Level View of our SET Tolerant Design

There was a 66mV reduction in the noise margin of an inverter in the protection logic due to our modified sizing approach. However, since this skewed sizing is *only* used in the secondary path, and all the nodes in the protection circuitry are SET immune based on the discussion of Section 3.2, this is not a problem. The functional path is not impacted by this skewed sizing.

It is important to note that in our approach, the Master latch of the system flip-flop needs to multiplex its input from the combinational logic (if there was no SET error) or from the CW^* signal in case there was a SET error. Instead of placing a MUX at its input, we fold the MUX into the Master latch itself. This results in a minimal delay penalty. The modified Master latches used in the RAZOR approach [28, 29, 30] add a MUX in the critical delay path instead.

3.4 Timing Analysis

The maximum width of a SET glitch that can be protected by our SET protection scheme is determined as the minimum of two quantities ($D_{min}/2$ and $1/2(D_{max}-\Delta)$). This section provides the timing analysis to derive these two conditions.

The first quantity which determines the maximum tolerable SET glitch is $D_{min}/2$. In Figure 4*b*), consider an SET glitch of width δ at the D input of the system flip-flop (DFF_modified). Let us assume that the glitch begins just before the rising edge of *CLK*. In an unprotected circuit, this could have led to incorrect system evaluation. The input P^* to the CWSP element is at its correct value after time δ. The second input to the CWSP element attains its correct value after an additional delay of δ. Thus, the output of the CWSP element is guaranteed to be correct only after a delay of 2δ. Thus, the minimum delay D_{min} of the circuit must be greater than 2δ. Therefore, the maximum width of a SET induced glitch that can be protected by our approach is less than or equal to $D_{min}/2$. The value of δ used for the delay element is in fact slightly larger than the maximum glitch width that we intend to protect the circuit from.

$$\delta \leq D_{min}/2 \tag{2}$$

The *CW* signal attains its correct value after a delay of $2\delta + D_{CWSP}$, where D_{CWSP} is the delay of the CWSP element. An additional delay is introduced by the MUX with $EQGLB_F$ as the select signal. Thus, *CLK_DEL* should be delayed (compared to the system clock *CLK*) by:

$$delay\_for\_CLK\_DEL = 2\delta + D_{CWSP} + delay\_of\_MUX + T_{SETUP\_EQ} \tag{3}$$

where T_{SETUP_EQ} is the setup time of the Equivalence Checker design.

After *CLK_DEL* becomes high, if the *EQ* signal goes low, *EQGLB* is pulled low and the *CW* value is latched to CW^*. In the next clock cycle, CW^* would be used as the input for the system flip-flop. Thus, CW^* should attain its stable value before the next rising edge of the system clock *CLK*. Therefore, the minimum time period required for the design to protect a glitch of width δ is given by the right hand side of Equation 4

$$D_{max} + T_{SETUP\_SYS} + T_{CLK\_OUT\_SYS} \geq delay\_for\_CLK\_DEL + T_{CLK\_OUT\_EQ} + delay\_of\_AND1 + T_{CLK\_OUT\_DFF2} + T_{SETUP\_SYS} \tag{4}$$

where $T_{CLK\_OUT\_EQ}$, $T_{CLK\_OUT\_DFF2}$ and $T_{CLK\_OUT\_SYS}$ are the clock to output delays of the Equivalence Checker, DFF2 and the system flip-flop respectively. T_{SETUP_SYS} is the setup time for the system flip-flop. Note that we do not need to add the setup time for DFF2 in the right hand side of Equation 4, because *CW* attains its stable value before the rising edge of *CLK_DEL*. The left hand side of Equation 4 is the minimum duration of the system clock *CLK*, in terms of the maximum combinational delay D_{max}, the setup and clock-to-output times of the system flip-flop DFF_modified. This minimum system clock duration must be larger than the right hand side of Equation 4 for the output CW^* to be correctly latched in every clock cycle.

Using Equations 3 and 4, we can find the maximum size of the SET induced glitch δ that we can protect the circuit from. This is given by:

$$\begin{aligned}\delta &\leq 1/2(D_{max} - (T_{CLK\_OUT\_EQ} + T_{CLK\_OUT\_DFF2} + D_{CWSP} \\ &\quad - T_{CLK\_OUT\_SYS} + delay\_of\_MUX + T_{SETUP\_EQ} + delay\_of\_AND1)) \\ &= 1/2(D_{max} - \Delta)\end{aligned} \tag{5}$$

For a circuit with a given maximum delay D_{max}, Equation 5 can be used to find the value of the maximum SET induced glitch that the circuit can tolerate using our approach. If the clock period T is specified directly, then δ is given by

$$\begin{aligned}\delta \leq 1/2(T - (&T_{CLK\_OUT\_EQ} + T_{CLK\_OUT\_DFF2} + delay\_of\_MUX \\ &+ T_{SETUP\_SYS} + D_{CWSP} + T_{SETUP\_EQ} + delay\_of\_AND1))\end{aligned} \tag{6}$$

In order to compare our result with [13], we designed our circuits to tolerate glitches induced by an SET strike with charge Q = 100fC and 150fC and with τ_β = 50ps and τ_α = 200ps. These values of Q, τ_α and τ_β were experimentally simulated using SPICE [31], and found to cause glitches of widths 500ps and 600ps respectively when they strike a minimum-sized inverter. In order to protect the circuit from SET induced glitches of duration 500ps and 600ps, the circuit should have $D_{min} \geq$ 1000ps and 1200ps respectively (from Equation 2). It should also have a D_{max} value satisfying Equation 5.

Since the operation of our circuit critically depends on the clock, it is important to analyze the affect of clock skew. If there is a clock skew of amount '*s*', the effective D_{min} reduces by '*s*'. As per Equation 2, this will increase the constraint on δ as follows: $\delta \leq (D_{min} - s)/2$. The second constraint on δ (Equation 6) depends on the clock period, which will not be impacted by clock skew.

4 Experimental Results

The SET tolerance of our circuit structures was simulated in SPICE [31]. We used a 65nm BPTM [32] model card, with $VDD = 1V$ and $V_{T_N} = |V_{T_P}| = 0.22V$. The benchmark circuits for our simulations were chosen from the LGSynth93 and the ITC design suites.

	Area Overhead			Delay Overhead			
Circuit	Regular (μm^2)	Hardened (μm^2)	%Ovh.	D_{max} (ps)	Regular (ps)	Hardened (ps)	%Ovh.
alu2	28.251025	37.292225	32.00	1624.53789	1733.53789	1745.03789	0.66
alu4	53.87795	65.87735	22.27	1700.28379	1809.28379	1820.78379	0.64
apex2	399.67155	404.27545	1.15	2069.548209	2178.548209	2190.048209	0.53
C3540	97.8256	130.5324	33.43	1931.05049	2040.05049	2051.55049	0.56
C6288	223.594225	271.092025	21.24	5141.05603	5250.05603	5261.55603	0.22
seq	421.598	473.5331	12.32	2936.803	3045.803	3057.303	0.38
C7552	187.676175	347.624775	85.23	2472.79124	2581.79124	2593.29124	0.45
C880	36.15365	74.77685	106.83	1692.79889	1801.79889	1813.29889	0.64
Average			39.31				0.51

Table 1: Area and Delay Overhead of Our Circuit Protection Approach for $Q = 0.15pC$, $\tau_\alpha = 200ps$ and $\tau_\beta = 50ps$

	Area Overhead			Delay Overhead			
Circuit	Regular (μm^2)	Hardened (μm^2)	%Ovh.	D_{max} (ps)	Regular (ps)	Hardened (ps)	%Ovh.
alu2	28.251025	36.380825	28.78	1624.53789	1733.53789	1745.03789	0.66
alu4	53.87795	64.66215	20.02	1700.28379	1809.28379	1820.78379	0.64
apex2	399.67155	403.81975	1.04	2069.548209	2178.548209	2190.048209	0.53
C1908	43.660325	77.006925	76.38	1562.64811	1671.64811	1683.14811	0.69
C3540	97.8256	127.1906	30.02	1931.05049	2040.05049	2051.55049	0.56
C6288	223.594225	266.231225	19.07	5141.05603	5250.05603	5261.55603	0.22
C7552	187.676175	331.219575	76.48	2472.79124	2581.79124	2593.29124	0.45
C880	36.15365	70.82745	95.91	1692.79889	1801.79889	1813.29889	0.64
seq	421.598	468.2166	11.06	2936.803	3045.803	3057.303	0.38
C5315	152.169625	315.630825	107.42	1475.91072	1584.91072	1596.41072	0.73
dalu	65.594625	86.996425	32.63	1489.08672	1598.08672	1609.58672	0.72
Average			45.34				0.56

Table 2: Area and Delay Overhead of Our Circuit Protection Approach for $Q = 0.10pC$, $\tau_\alpha = 200ps$ and $\tau_\beta = 50ps$

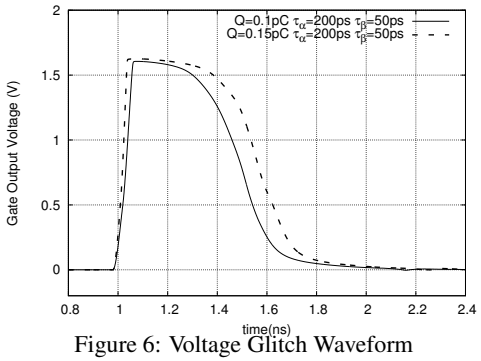


Figure 6: Voltage Glitch Waveform

The radiation strike was modeled as a current source described as $I(t) = \frac{Q}{(\tau_\alpha - \tau_\beta)}(e^{-t/\tau_\alpha} - e^{-t/\tau_\beta})$.

In order to compare our results with [13], the first set of experiments were done using a value of $\tau_\beta = 50ps$, $\tau_\alpha = 200ps$ and $Q = 100fC$ and $150fC$. We first compute the width of the voltage glitch when a charge of this value strikes a minimum-sized inverter. The results from this simulation are shown in Figure 6. Note that the voltage of the node rapidly rises, before saturating at 1.6V. This occurs due to the turning on of junction diodes in the devices (which turn on at ~0.6V above VDD). We note that the resulting maximum glitch widths are 500ps and 600ps (for $Q = 100fC$ and $150fC$ respectively).

Based on this information, we know that for our SET protection scheme to work, we should utilize delay elements whose delay value δ (for delaying the D signal of DFF_modified) and $2\delta + D_{CWSP} + T_{SETUP\_EQ}$ (for deriving CLK_DEL). The delay circuit was constructed by connecting a high resistivity POLY2 wire in series with the input of a minimum-sized inverter (with its PMOS device width equal to the width of the NMOS device). We define one POLY2 resistor followed by an inverter as a *segment*. For $Q = 100fC$, we required 4 segments to achieve a delay δ, and 8 segments to implement the delay element for *CLK_DEL*. For $Q = 150fC$, we used 4 and 10 segments to achieve a delay of δ and *CLK_DEL* respectively. We were able to obtain a higher delay with 4 segments for $Q = 150fC$ compared to $Q = 100fC$ by increasing the value of the POLY2 resistors used. Note that the delay element can be modified to provide different values of delay by either changing the number of segments or the value of the resistors. The value of the resistors is limited since we require that the output of the resistors transition between *VDD* and *GND* within the required delay.

Also, the CWSP element of our design should be SET tolerant for voltage glitches induced by $Q = 100fC$ and $150fC$. The exercise of determining the sizing of the CWSP devices was conducted via SPICE [31] simulations. The CWSP element for 100fC SET tolerance was sized 30/12[3]. For 150fC SET tolerance, the CWSP element was sized 40/16.

The remaining transistors in Figure 5 were all custom sized, and their correct operation was validated in SPICE.

[3]A size of X/Y indicates that all the PMOS devices were X times minimum sized, and the NMOS devices were Y times minimum

According to the timing analysis discussion of Section 3.4, in order to protect a glitch of maximum width δ, the minimum value of D_{max} can be computed using Equation 4. The only variable quantity in this equation is the $delay\_of\_AND1$. For a 30-input NOR gate, to protect a circuit from glitches of widths 500ps and 600ps, this minimum value of D_{max} was found to be 1415ps and 1605ps respectively. For the testcases with more than 30 outputs, a multi level gate was used to confirm that the D_{max} constraint is being met.

Table 1 shows the delay and area overheads associated with our approach, for several examples. This table shows the overheads for an SET tolerance of up to 150fC. Column 1 describes the circuit under consideration. Columns 2 and 3 report the active area in μm^2 for regular design and a design hardened by our approach. Column 4 reports the percentage area overhead of using our approach. Column 5 provides the D_{max} value for the circuits. As required, all the testcases in Table 1 have a *Dmax* value greater than 1605ps. Columns 6 and 7 report the delays for a regular design and a design hardened with our approach. Column 8 reports the percentage delay overhead of our approach. Table 2 shows corresponding results for Q = 100fC.

As per [33], industrial circuits are typically balanced to have roughly equal longest and shortest path lengths. This is done in order to avoid hold-time violations. State of the art technology mapping tools ensure that the D_{min} is about 80% of D_{max} [33]. Based on this, taking D_{min} to be 80% of D_{max}, we note that $\delta \leq D_{min}/2$ constraint is satisfied for all the circuits in Table 1 and Table 2.

The SET tolerant portion of our design is not in the critical path of the system computation. It is sized carefully, so as to add minimal parasitic capacitances to the system flip-flop delay path. Based on our simulations, the *CLK*-to-*Q* delay increased to 76ps using our approach (compared to 69ps). However, the setup time decreased by 2ps (from 40ps to 38ps) using our approach. Additionally, the increased load on the D input of the Master system latch resulted in an increase in the delay (by 6.5ps) of the combinational output of the design. As a consequence, the total delay penalty associated with adding our SET tolerant circuit is 11.5ps per flip-flop. These values have been used to calculate the delays as per the left hand side of equation 4. For the protected case, the extra 6.5ps due to the increased load on the D input of the Master system latch (explained above) was also included.

The difference in our SET protection circuit (Figure 4) for $Q = 100fC$ and $150fC$ is the delay element and the size of the CWSP element. The path through the system flip-flop remains unaltered. Therefore, the delay penalty in both the cases is same. Based on the results in Table 1 and Table 2, we note that our approach has an average area overhead of 45.34% (39.31%) for $Q = 150fC$ ($Q = 100fC$). However, the corresponding delay penalty is 0.56% (0.51%) which is extremely small. Hence, our SET protection approach has a negligible delay penalty.

Table 4 summarizes our results in comparison to the results of [13] and [15]. The approach of [13] reports average area overheads which are comparable, and larger average delay overheads (about 2.8%). Also, the approach of [13] provides 90% protection to SET induced glitches, while our approach provides 100% protection. For high speed, mission critical applications, the reduced delay of our scheme could be extremely crucial, especially when it comes with a no additional area penalty compared to [13]. In [15], the calculated average area overheads were about 17.6%. However, the average delay penalty was quite substantial

	Area Overhead			Delay Overhead				Max. Glitch Width
Circuit	Regular (μm^2)	Hardened (μm^2)	%Ovh.	D_{max} (ps)	Regular (ps)	Hardened (ps)	%Ovh	δ (ps)
apex4	200.0291	225.4125	12.69	1396.654	1505.654	1517.154	0.76	491
apex3	139.1276	208.5942	49.93	1230.121789	1339.121789	1350.621789	0.86	408
b11_opt_C	55.428075	104.701075	88.90	1270.94562	1379.94562	1391.44562	0.83	428
C1355	46.009025	88.646025	92.67	1012.19256	1121.19256	1132.69256	1.03	300
C432	15.120875	24.577875	62.54	1385.38584	1494.38584	1505.88584	0.77	485
C499	46.009025	88.646025	92.67	1012.19256	1121.19256	1132.69256	1.03	300
ex5p	178.177325	264.897525	48.67	1195.07966	1304.07966	1315.57966	0.88	390
k2	88.5317	151.3623	70.97	1170.34338	1279.34338	1290.84338	0.90	378
apex1	111.4312	174.2618	56.39	982.903	1091.903	1103.403	1.05	284
ex4p	17.594425	24.397025	38.66	630.381	739.381	750.881	1.56	108
Average			61.41				0.99	

Table 3: Area and Delay Overhead of Our Circuit Protection Approach for glitch width up to $\delta = min\{D_{min}/2, (D_{max} - \Delta)/2\}$

(28.65%). Therefore, our approach provides an attractive design point.

Technique	Area Overhead (%)	Delay Overhead (%)	Protection
Our Approach	42.33	0.54	100%
[13]	42.95	2.80	90%
[15]	17.60	28.65	100%

Table 4: Summary of our results compared to the approach of [13] and [15]

For the cases in which D_{max} is less than 1415ps (corresponding to $Q = 100fC$), we can still protect against SET induced glitches of width up to $min\{D_{min}/2, (D_{max} - \Delta)/2\}$. To achieve this, in the circuit for our SET protection scheme shown in Figure 4, the delay element needs to be changed to a value $\delta = min\{D_{min}/2, (D_{max} - \Delta)/2\}$. This can be achieved by reducing the value of the POLY2 resistors used for the delay element, or by reducing the number of segments used to construct the delay elements. Also, the CWSP element can be made smaller as well, since it needs to tolerate a glitch of lesser width (compared to $Q = 100fC$). In Table 3, we have used the area of our SET protection circuit for $Q = 100fC$ to compute the area overhead. Note that this is an upper bound on the actual area overhead achievable. To find out the maximum width of the SET induced glitch (δ) that our technique can protect these circuits against ($min\{D_{min}/2, (D_{max} - \Delta)/2\}$), D_{min} was taken to be 80% of D_{max} [33]. We used the same value of Δ as was used for the experiments with $Q = 100fC$, which was equal to 415ps. All other columns in this table have the same meaning as the columns of Tables 1 and 2. The delay overhead is calculated in the manner discussed earlier in this section. It can be seen that the delay overhead is minimal (0.99%) with an area overhead of 61.41%. Note that this area overhead is an overestimate of the true area overhead.

5 Conclusion

In this paper, we present a novel radiation-hardened digital design approach. This approach uses Code Word State Preserving (CWSP) elements at each flip-flop of the design, leaving the rest of the design unaltered. Since the CWSP elements are connected off the critical delay path in the design, our SET tolerant approach has negligible delay overheads. Our CWSP based approach provides 100% protection for SET induced glitches of widths up to $min\{D_{min}/2, (D_{max} - \Delta)/2\}$. In case an SET error is detected, then the current computation is repeated, using the correct output, which is generated later in the same clock period by the CWSP element. The CWSP logic is designed to minimally impact the critical delay path of the design, with a delay penalty (averaged over several designs) of less than 1%. Thus our technique is applicable for high-speed designs, where the additional delay associated with SET protection must be kept at a minimum.

References

[1] Q. Zhou and K. Mohanram, "Transistor sizing for radiation hardening," in *Proc. International Reliability Physics Symposium*, pp. 310–315, apr 2004.

[2] A. Johnston, "Scaling and technology issues for soft error rate," in *Proc. Annual Research Conference on Reliability*, oct 2000.

[3] M. Caffrey, P. Graham, E. Johnson, and M. Wirthli, "Single-event upsets in SRAM FPGAs"," in *Proc. International Conference on Military and Aerospace Programmable Logic Devices*, sep 2002.

[4] C. Carmichael, E. Fuller, M. Caffrey, P. Blain, and H. Bogrow, "SEU mitigation techniques for virtex FPGAs in space applicaions," in *Proc. International Conference on Military and Aerospace Programmable Logic Devices*, sep 1999.

[5] T. Speers, J. Wang, B. Cronquist, J. McCollum, H. Tseng, R. Katz, and I. Kleyner, "0.25pm flash memory based FPGA for space application," in *Proc. International Conference on Military and Aerospace Programmable Logic Devices*, sep 1999.

[6] B. Gill, M. Nicolaidis, F. Wolff, C. Papachristou, and S. Garverick, "An efficient BICS design for SEUs detection and correction in semiconductor memories," in *Proceedings, Design, Automation and Test in Europe*, pp. 592–597, march 2005.

[7] W. Massengill, M. Alles, and S. Kerns, "SEU error rates in advanced digital CMOS," in *Proc. Second European Conference on Radiation and its Effects on Components and Systems*, pp. 546 – 553, sep 1993.

[8] J. Pickle and J. Blandford, "CMOS RAM cosmic-ray-induced error rate analysis," *IEEE Trans. on Nuclear Science*, vol. NS-29, pp. 3962–3967, 1981.

[9] K. Hass and J. Gambles, "Single event transients in deep submicron CMOS," in *Proc. IEEE 42nd Midwest Symposium on Circuits and System*, pp. 122–125, 1999.

[10] W. Beauvais, P. McNulty, W. A. Kader, and R. Reed, "SEU parameters and proton-induced upsets," in *Proc. Second European Conference on Radiation and its Effects on Components and Systems*, pp. 54–545, sept 1993.

[11] G. Messenger, "Collection of charge on junction nodes from ion tracks," *IEEE Trans. Nuclear Science*, vol. 29, no. 6, pp. 2024–2031, 1982.

[12] A. Dharchoudhury, S. Kang, H. Cha, and J. Patel, "Fast timing simulation of transient faults in digital circuits," in *Proc. IEEE/ACM International Conference on Computer-Aided Design*, pp. 719–726, Nov 1994.

[13] Q. Zhou and K. Mohanram, "Gate sizing to radiation harden combinational logic," in *Proceedings, Computer-Aided Design of Integrated Circuits and Systems*, pp. 155–166, Jan 2006.

[14] D. Mavis and P. Eaton, "Soft error rate mitigation techniques for modern microcircuits," pp. 216–225, 2002.

[15] L. Anghel, D. Alexandrescu, and M. Nicolaidis, "Evaluation of a soft error tolerance technique based on time and/or space redundnacy," in *Proceedings, 13th Symposium on Integrated Circuits and Systems Design*, pp. 237–242, 2000.

[16] S. Mitra, N. Seifert, M. Zhang, and K. Kim, "Robust system design with built-in soft-error resilience," *IEEE Computer*, pp. 43–52, Feb 2005.

[17] E. Fuller, M. Caffrey, A. Salazar, C. Carmichael, and J. Fabula, "Radiation testing update, SEU mitigation, and availability analysis of the Virtex FPGA for space reconfigurable computing," in *Proc. International Conference on Military and Aerospace Programmable Logic Devices*, sep 2000.

[18] J. Wang, B. Cronquist, and J. McGowan, "Rad-hard/hi-rel FPGA," in *Proc. of the Third ESA Electronic Components Conference*, apr 1997.

[19] T. May and M. Woods, "Alpha-particle-induced soft errors in dynamic memories," *IEEE Trans. on Electron Devices*, vol. ED-26, pp. 2–9, jan 1979.

[20] G. Agrawal, L. Massengill, and K. Gulati, "A proposed SEU tolerant dynamic random access memory (DRAM) cell," in *IEEE Transactions on Nuclear Science*, vol. 41, pp. 2035–2042, Dec 1994.

[21] M. Nicolaidis, "Time redundancy based soft-error tolerance to rescue nanometer technologies," in *VLSI Test Symposium*, pp. 86–94, April 1999.

[22] Q. Zhou and K. Mohanram, "Transistor sizing for radiation hardening," in *Proceedings, Reliability Physics Symposium Proceedings*, pp. 310–315, 2004.

[23] M. Nicolaidis, "Time redundancy-based soft-error tolerance to rescue nanometer technologies," in *Proceedings, IEEE VLSI Test Symposium*, pp. 86–94, 1999.

[24] R. Garg, N. Jayakumar, S. Khatri, and G. Choi, "A design approach for radiation-hard digital electronics," in *DAC '06: Proceedings of the 43rd annual conference on Design automation*, pp. 773–778, ACM Press, 2006.

[25] J. Rabaey, *Digital Integrated Circuits: A Design Perspective*. Prentice Hall Electronics and VLSI Series, Prentice Hall, 1996.

[26] E. E. C. for Space Standardization, "Energetic Particle Radiation, http://www.spenvis.oma.be/spenvis/ecss/ecss09/ecss09.html."

[27] J. Feynman, G. Spitale, J. Wang, and S. Gabriel, *Interplanetary Proton Fluence Model: JPL 1991*. J. Geophys. Res. 98, A8, 1993.

[28] S. Das, S. Pant, D. Roberts, S. Lee, D. Blaauw, T. Austin, T. Mudge, and K. Flautner, "A self-tuning DVS processor using delay-error detection and correction," *Journal of VLSI Circuits*, pp. 258–261, Jun 2005.

[29] S. Das, D. Roberts, S. Lee, S. Pant, D. Blaauw, T. Austin, T. Mudge, and K. Flautner, "A self-tuning dynamic voltage scaled processor using delay-error detection and correction," pp. 792–804, Apr 2006.

[30] D. Ernst, N. S. Kim, S. Das, S. Pant, R. Rao, T. Pham, C. Ziesler, D. Blaauw, T. Austin, K. Flautner, and T. Mudge, "Razor: a low-power pipeline based on circuit-level timing speculation," in *International Symposium on Microarchitecture*, pp. 7–18, Dec 2003.

[31] L. Nagel, "Spice: A computer program to simulate computer circuits," in *University of California, Berkeley UCB/ERL Memo M520*, May 1995.

[32] Y. Cao, T. Sato, D. Sylvester, M. Orshansky, and C. Hu, "New paradigm of predictive MOSFET and interconnect modeling for early circuit design," in *Proc. of IEEE Custom Integrated Circuit Conference*, pp. 201–204, Jun 2000. http://www-device.eecs.berkeley.edu/ ptm.

[33] W. K. C. Lam, R. K. Brayton, and A. L. Sangiovanni-Vincentelli, "Valid clock frequencies and their computation in wavepipelined circuits," *Computer-Aided Design of Integrated Circuits and Systems*, vol. 15, no. 7, pp. 791–807, 1996.