Auto-tuning Fault Tolerance Technique for DSP-Based Circuits in Transportation Systems

Ihsen Alouani, Smail Niar, Yassin El-Hillali, and Atika Rivenq

[1] I. Alouani and S. Niar LAMIH lab
University of Valenciennes
France
firstname.name@univ-valenciennes.fr
[2] Y. El-Hillali and A. Rivenq IEMN lab
University of Valenciennes
France
firstname.name@univ-valenciennes.fr

Abstract. As new technologies use a reduced transistor size to improve performance, circuits are becoming remarkably sensitive to soft errors that become a serious threat for critical applications reliability. Most of the existing reliability enhancing techniques lead to costly hardware. The masking phenomenon is fundamental to accurately estimating soft error rates (SER). The first contribution of this paper is a new cross-layer model for input-dependent Single Event Transient (SET) masking mechanisms combining Transistor Level Masking (TLM) and System Level Masking (SLM). We, secondly, use this model to build an auto-tuning fault tolerant circuit dedicated to obstacle detection systems in railway transportation. Based on our input-dependent masking model, the proposed architecture evaluates the effective circuit's vulnerability at runtime and accordingly adapts the reliability boosting strategy, leading to a reliable circuit with optimized overheads. When compared to the Triple Modular Redundancy, our technique reduces the number of FPGA LUTs (resp. DSP slices) by up to 45% (resp. 33%).

1 Introduction and Related Works

Technology scaling has enabled fabulous improvements in embedded systems performance. Nevertheless, as transistor gate dimensions decrease to the nanometer scale, electronic systems become highly susceptible to environmental-factors-induced errors. Soft errors are caused by particle strikes that temporarily corrupt data stored in memory cells, or change the state of internal combinational circuit nodes. The masking phenomenon is one of the most important fundamentals involved in failure rates estimation within semiconductor circuits. In the existing works, three masking mechanisms preventing combinational circuits from soft errors have been considered [1]: Logical Masking, Electrical Masking and Latching-Window Masking. The most widely used reliability enhancement techniques in the literature are: *spatial* redundancy and *temporal* redundancy.

In this paper, we present ARDAS for *Auto-tuning Redundancy in DSP-based Architectures for Soft errors resiliency*, an architecture that uses auto-tuning redundancy of DSP blocks to protect the vulnerable circuit parts instead of protecting the whole circuit. The vulnerability analysis is performed through design-time simulations that implement the proposed masking models (TLM and SLM).

2 TLM: Transistor-Level Masking Mechanism

TLM occurrence is led by the affected transistor locality within the struck gate as well as the input combination during the transient event. In fact, the particle strike temporarily corrupts combinational elements by affecting the state of the hit transistor. However, the event can be simply unnoticed at the output if the transistor behavior corruption doesn't affect the overall state of pull-up/pull-down network. Let be D_i a binary variable set to 1 if the error due to a particle strike hitting a transistor Q_i is masked by a TLM mechanism. P_i is the probability that Q_i is the hit transistor within the struck gate by the particle. Hence, the probability that the error resulting from a radiation strike in gate j is masked for a given input combination in gate j is then expressed by: $P_{TLM}(j) = \sum_{i=1}^{N_j}(P_i \times D_i)$. For simplicity, we assume the equiprobability of gates' transistors to be hit by a particle. Let N_m be the number of cases the error is masked for a given input combination. Hence, $P_{TLM}(j) = \frac{N_m}{N_j}$.

The probability of soft error masking in the output bit S_i of a combinatorial circuit for given input signals is:

$$P^i_{masking} = \sum_{j=1}^{n} W_j \cdot (P_{TLM}(j) + (1 - P_{TLM}(j)) \cdot D_{ij}) \quad (1)$$

Where n is the number of gates in the circuit, $P_{TLM}(j)$ is the probability of TLM at gate j and W_j is the weight assigned to gate j, expressed as the number of the gate's transistors divided by the total number of transistors in the circuit. Finally, D_{ij} is a binary variable set to 1 if the error at gate j does not propagate to output S_i and to 0 otherwise.

3 SLM: System-Level Masking Mechanism

In a threshold-based system, the comparison of the intermediate result with a beforehand fixed threshold gives the overall system decision. A transient error in the intermediate result may keep the overall system decision unchanged depending on the detection threshold value.

We consider a widely used signal processing element in detection/recognition applications, namely a correlator. We built a simulation tool that tracks the propagation of event-induced errors happening within the correlator nodes and evaluated their impact on obstacle detection accuracy. The correlator is implemented using DSP48E1 slices [2]. A soft error is modeled by injecting a bit flip in a node (i, j) corresponding to the output bit i of the DSP_j. Hence, the system behavior can be monitored under fault injection through *System Failures* (SFs) detection. A SF corresponds either to a "False Alarm", or a "No Alarm". To identify SFs, we introduce the variable δ_{ij} that is expressed by: $\delta_{ij} = ({C_{ij}}^* - Y_0) \cdot (C - Y_0)$, where ${C_{ij}}^*$ is the correlation result under fault injection in node (i, j), C is the error-free result and Y_0 is the correlation threshold. A SF occurs when $\delta_{ij} < 0$. However, if $\delta_{ij} \geq 0$ we have a System Level Masking (SLM).

4 ARDAS: Proposed Approach

We define V_j, the vulnerability of a DSP_j by:

$$V_j = \frac{\sum_{i=1}^{N_j} \eta_{ij} \cdot (1 - P_{ij})}{N_j} \tag{2}$$

Where: N_j is the number of output bits of DSP_j, P_{ij} is the probability of TLM relative to bit i of DSP_j and η_{ij} is a variable set to 0 if a fault at node (i, j) is masked by SLM, i.e. $\delta_{ij} \geq 0$ and is equal to 1 otherwise. We localize vulnerable DSPs as those with $V_j > V_0$ and define α_j as follows: $\alpha_j = 0$ if $V_j > V_0$ and $\alpha_j = 1$ if $V_j \leq V_0$. As $[V_j]$ vector depends on the applied input signals, the redundancy distribution corresponding to the vulnerability map has to be dynamically tunable and self adaptive. The main idea is to judiciously use the redundant DSP slices to carry out an auto-tuning partial TMR instead of a full TMR. The system adapts the redundancy to the actual vulnerability map of the circuit using the circuit's $[\alpha_j], \forall j \in [1; N_{dsp}]$.

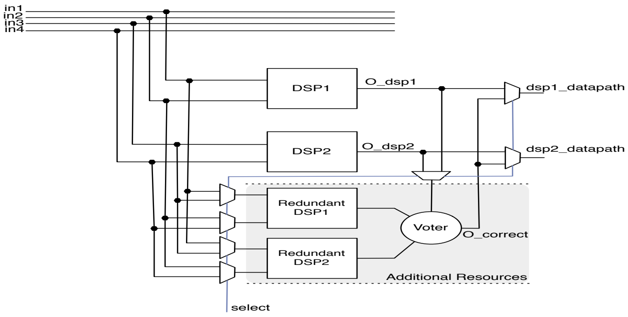

Fig. 1. An illustrative circuit of the auto-tuning redundancy used in ARDAS

The reconfiguration process used to change the redundancy mapping at run-time is taken from our previous work [3] and an example is illustrated in Figure 1. The circuit mapping is configured by a single control word according to a redundancy map obtained offline through design-time simulations.

5 Experimental Results

We compare the SER of ARDAS-protected to a TMR-protected correlation circuit. As the reliability level is tuned via V_0, Figure 2 represents the normalized SER and the number of used DSP slices in ARDAS in terms of the tolerated DSP vulnerability threshold. As seen in Figure 2, the reliability level provided by ARDAS is comparable to TMR reliability level with lower HW resource utilization.

Table 1. Resource utilization, power and maximum frequency.

	Original	TMR	ARDAS V_0=0.55	ARDAS V_0=0.7	DTR
DSPs	79	237	189	159	79
LUTs	0	1798	1619	1207	1413
Pw(mW)	430	691	542	533	459
Max freq (MHz)	422	247	347	347	410

In addition to the reliability, we investigate the impact of ARDAS on power consumption, resource utilization and the maximum clock frequency of each circuit for two vulnerability threshold values: 0.55 and 0.7. The circuit is synthesized for a Xilinx Virtex 7 board. The power consumption is estimated using the Xilinx XPower Analyser tool. Table 1 shows that our architecture reduces the reliability cost in terms of resource utilization, power and performance. In fact, ARDAS decreases the number of used LUTs by 10% for $V_0 = 0.55$ and by 32% for $V_0 = 0.7$ compared to TMR. On the other hand, while using TMR slows

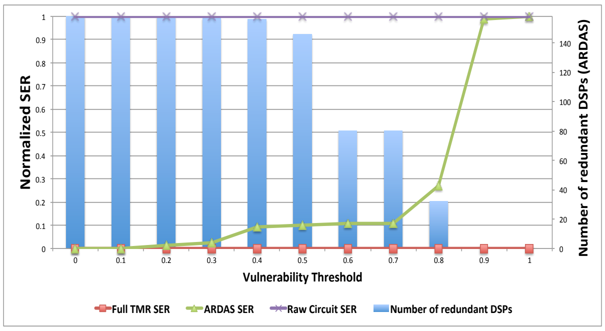

Fig. 2. Normalized SER (left axis), used DSP resources vs V_0 (right axis)

down the circuit frequency by 42%, ARDAS performance penalty is less than 18% compared to the unprotected circuit.

6 Conclusion

In this paper, a self adaptive reliability approach is proposed to cope with the increasing error rates in new technologies with the lowest possible overheads. ARDAS relies on an auto-tuning redundancy architecture to protect the vulnerable parts of the system rather than the whole circuit. Due to its quick reconfigurability, ARDAS offers high reliability with reduced overheads. Moreover, it allows designers to choose the desired reliability level depending on the application requirements and its criticality.

References

1. P. Dodd and L. Massengill, "Basic mechanisms and modeling of single-event upset in digital microelectronics," *IEEE Tran onNuclear Science*, June 2003.
2. 7 series dsp48e1 slice user guide. [Online]. Available: www.xilinx.com/support/documentation/user-guides/ug479-7Series-DSP48E1.pdf
3. I. Alouani, M. A. R. Saghir, and S. Niar, *Reconfigurable Computing: Architectures, Tools, and Applications: 10th International Symposium, ARC 2014, Vilamoura, Portugal, April 14-16, 2014. Proceedings*, ch. ARABICA: A Reconfigurable Arithmetic Block for ISA Customization, pp. 248–253.