Low power probabilistic online monitoring of systematic erroneous behaviour

Gutierrez, M.D., Tenentes, V., Kazmierski, T.J. and Rossi, D.

Low Power Probabilistic Online Monitoring of Systematic Erroneous Behaviour

Mauricio D. Gutierrez, Vasileios Tenentes, Tom J. Kazmierski
University of Southampton, UK
Email: {mdga1g11, V.Tenentes, tjk}@ecs.soton.ac.uk

Daniele Rossi
University of Westminster, UK
D.Rossi@westminster.ac.uk

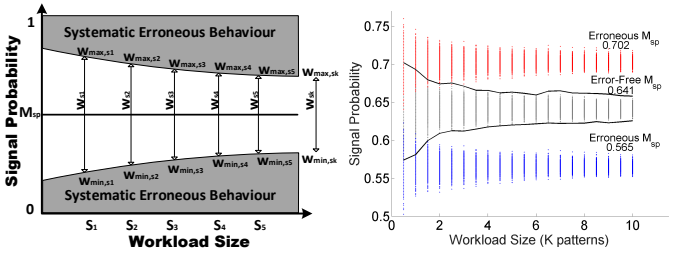
***Abstract*—Electronic devices with power-constrained embedded systems are used for a variety of IoT applications, such as geo-monitoring, parking sensors and surveillance, which may tolerate few errors and may not be constrained by a strict error detection latency requirement. In this poster, we propose a novel low power online error monitoring technique that produces an alarm signal when systematic erroneous behaviour has occurred over a pre-defined time interval. A monitoring architecture monitors the signal probabilities of the logic cones concurrently to its normal operation and compares them on-chip against the signature of error-free behaviour. Results on a set of the EPFL'15 benchmarks show an average error coverage of 82.9%% of errors induced by stuck-at faults, with an average area cost of 1.2% and an error detection latency of [0.01, 3.3] milliseconds.**

I. Introduction

Intermittent faults at circuits manufactured using Very Deep Sub-Micron (VDSM) technologies manifest as bursts of errors that repeat periodically at the same places [1], causing the circuit to exhibit systematic erroneous behaviour (SEB). Devices in the field that exhibit SEB must be identified and maintained. However, the maintenance of electronic devices used in low-power IoT applications requires often physical access which might be impractical and has to be planned in advance. Thus, the maintainability of those devices can be assisted by monitoring their behaviour in-the-field. As a result, a low power solution for monitoring SEB online is required. Many applications for low power embedded devices such as geo-monitoring, parking sensors, or surveillance, may tolerate some errors [2]. Such devices are not constrained by a strict error detection latency requirement, thus detecting errors immediately as they occur may not be required, as long as they continue to offer their intended service. However, being able to quantify the amount of erroneous behaviour exhibited by each device, would be beneficial for maintainability purposes.

II. Analysis of online signal probabilities

Figure 1a presents the concept of online signal probabilities (OSPs). The number of input patterns in a workload is referred to as workload size, denoted by S. In error-free normal operation, the OSPs at a given node may vary depending on the workload. As the S increases, the variation of the OSP decreases and it starts to converge. The value to which the OSP converges is the *mean signal probability*, denoted by M_{sp}. The variation of the OSP during an error-free operation is referred to as *signature window* (w), with W_{max} and W_{min} as the *upper and lower bounds*. The expected M_{sp} and w



(a) (b)

Fig. 1: (a) Concept of Online signal probabilities, (b) Online signal probabilities of 1000 workloads for circuit t481

are dependent on the input signal probabilities. Systematic erroneous behaviour (SEB) is defined as the event in which, for a particular workload size S, systematic errors occur at a high enough rate that the OSP of an output falls outside the signature window w. SEB may occur in-the-field due to intermittent faults that manifest periodically as *multiple bit-flips* or exhibit a behaviour similar to *permanent faults* under specific operating conditions [1]. When such a fault is activated, it may generate enough errors that the OSP falls outside the signature window bounds.

Example: The t481 circuit of the LGSynth'91 benchmarks consists of a single logic cone of 388 gates with 16 inputs and 1 output. The error-free (grey) and erroneous (red and blue) online signal probabilities of 1000 different unbiased workloads, each of them consisting of 10K input patterns, are shown in Figure 1b. The mean online signal probability M_{sp} of the error-free case is 0.641. When the circuit exhibits SEB, the OSP converge to different values than the error-free M_{sp}.

Figure 2a shows that the OSP of an error-free workload execution follows a normal distribution, which can be modelled. Computing the mean value and the standard deviation σ of the normal distribution, we can select appropriately the w to avoid false alarms. For instance, approximately 99.7% of the error-free OSP are within a signature window w=$[M_{sp} \pm 3\sigma]$, 95.5% are within a w=$[M_{sp} \pm 2\sigma]$, and 68.3% are within a w=$[M_{sp} \pm \sigma]$. Thus, the probability of having a false alarm is a function of the selected window, which corresponds to 0.3%, 4.5% and 31.7% for the windows w=$[M_{sp} \pm 3, 2, 1\sigma]$ respectively. Figures 2b and 2c present the histograms of OSP for faults and errors, respectively, after performing a full single stuck-at (SSA) fault injection campaign. The SSA fault model is used to emulate intermittent faults causing

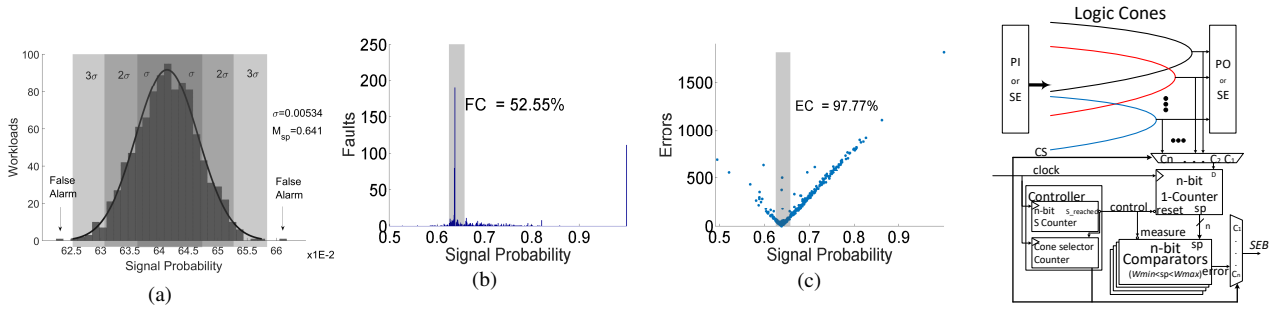


Fig. 2: (a) Error-free Normal Distribution, (b) OSP of stuck-at faults and (c) propagated errors for circuit t481 with $w = M_{sp} \pm 3\sigma$. (d) Proposed monitoring architecture

SEB in-the-field [1]. The horizontal axis shows the OSP and the vertical axis shows the number of injected faults that exhibit the corresponding OSP. An unbiased workload of size $S = 5000$ was used and the signature window was defined as w=$[M_{sp} \pm 3\sigma]$, with $\sigma = 0.00534$. The fault coverage (FC) of 52.55% is calculated by counting all the SSA faults that cause the OSP to fall outside the w. Not all faults present during normal operation bypass the inherent logic masking of a circuit [3]. When fault is masked, few errors are propagated with a small effect in the OSPs. That FC indicates that 47.45% of the SSA faults have a small impact on the OSP. The error coverage (EC) is defined as the number of error propagated by each injected fault and whose OSP falls outside the signature window, divided by the total number of errors. The resulting EC of 97.77% implies that most errors observed at the output are associated to an OSP that deviates significantly from the mean signal probability M_{sp}

Monitoring architecture: The monitor design (Fig. 2d) consists of a *n-bit counter* that increases on the rising edge of the clock when the input *D* is asserted, counting the number of logic 1's. The *n-bit comparators* assert the *SEB* output if the signal probability *sp* coming from the counter is outside the $Wmin$ and $Wmax$ values when the inverted *measure* input is deasserted. The measure input is deasserted when the *S counter* in the controller has counted S clock cycles. This signal also increases the *Cone selector counter*, whose output *CS* selects which cone to monitor in a round-robin fashion.

III. Simulation Results

This technique was evaluated for errors induced by stuck-at faults, as these faults produce a behaviour similar to long duration intermittent faults [1]. Random workloads of various sizes were applied during simulations. Single stuck-at injection simulation of all possible faults sites is performed to calculate the EC of errors induced by single stuck-at faults (ibSSA).

Table I presents the results after monitoring a few logic cones of some of the EPFL'15 benchmarks. The third column shows the error detection latency (EDL) given by the workload size S followed by the number of monitored cones $[1, 5, 10, 15]$. The ibSSA EC of the selected cones and of the whole circuit is shown next, followed by the area cost of the monitoring architecture. Monitoring the logic cone that exhibits the most errors using a signature window $w = M_{sp} \pm \sigma$,

TABLE I:
ibSSA Error Coverage and Area Cost

Benchmark	Circuit Size (Gates)	Workload Size S / EDL	Monitored Cones	ibSSA EC (%) $w = M_{sp} \pm \sigma$		Area Cost (%)
				Whole Circuit	Selected Cones	
sin	5416	7000	1	4.77	70.78	2.30
			5	26.80	71.51	2.98
			10	43.82	71.44	3.82
			15	56.44	70.53	4.67
log2	32060	10000	1	3.60	82.09	0.39
			5	19.25	74.88	0.50
			10	33.39	74.07	0.65
			15	43.78	72.93	0.79
voter	13758	10000	1	95.91		0.91

we see an average ibSSA EC of 82.9%, with an average area cost of 1.2%. An EDL estimation for these circuits can be performed by synthesizing them with a standard 90nm cell library using commercial tools. The resulting operating frequency is in the range of [3MHz, 1.1GHz], which produces an error detection latency in the range of [0.01, 3.3] milliseconds when detecting SEB after 10000 clock cycles.

IV. Conclusions

In this poster, we presented a novel technique for monitoring systematic erroneous behaviour online. We proposed the analysis of the online signal probabilities at the outputs of a circuit when the latter exhibits systematic erroneous behaviour and a monitoring architecture for observing the online signal probabilities at the outputs of the logic cones of a circuit. We evaluated the proposed technique on a set of EPFL'15 benchmark circuits achieving an average error coverage of 82.9% of errors induced by stuck-at faults, with an average area cost of 1.2% and an error detection latency in the range of [0.01,3.3] milliseconds.

Acknowledgments

This work has been supported by the Mexican CONACYT and by the EPSRC (UK) under grant no. EP/K034448/1.

References

[1] J. Gracia-Moran, J. C. Baraza-Calvo, D. Gil-Tomas, L. J. Saiz-Adalid, and P. J. Gil-Vicente, "Effects of intermittent faults on the reliability of a reduced instruction set computing (RISC) microprocessor," *IEEE Transactions on Reliability*, vol. 63, no. 1, pp. 144–153, 2014.

[2] Y. Qassim and M. E. Magana, "Error-tolerant non-binary error correction code for low power wireless sensor networks," *The International Conference on Information Networking 2014 (ICOIN2014)*, pp. 23–27.

[3] M. D. Gutierrez, V. Tenentes, and T. Kazmierski, "Susceptible workload driven selective fault tolerance using a probabilistic fault model," in *Proceeding on 22nd IEEE International Symposium on On-Line Testing and Robust System Design 2016.*