DESIGN DIVERSITY FOR REDUNDANT SYSTEMS

Subhasish Mitra, Nirmal R. Saxena and Edward J. McCluskey
Center for Reliable Computing
Stanford University, Stanford, California

ABSTRACT

Design diversity has long been known to protect redundant systems against common-mode failures. In this paper, for the first time, we present a metric to quantify diversity among several designs. Based on this metric, we derived analytical reliability models that show a simple relationship between design diversity, system failure rate, and mission time. In addition, we also present simulation results to demonstrate the effectiveness of design diversity in duplex and Triple Modular Redundant (TMR) systems. For independent multiple-module failures, both the analytical and simulation results show that there is no obvious advantage of using diversity in redundant systems. However, for common-mode failures, there is a significant gain in using diversity — however, the gain diminishes as the mission time increases. For a particular example, if the mission time goes down by a factor of 10, the reliability of a diverse system improves by more than a factor of 4 over a non-diverse system. Finally, our simulation results point out that diversity can enhance the self-testing properties of redundant systems.

1. INTRODUCTION

In any redundant system, *common-mode failures* (CMFs) result from failures that affect more than one module at the same time, generally due to a common cause. These include design mistakes and operational failures that may be externally caused (such as EMI, power-supply disturbances and radiation) or internal. *Design diversity* has been proposed in the past to protect redundant systems against common-mode failures [Avizienis 84][Lala 94] and has been used in both hardware and software systems [Riter 95][Avizienis 77]. The basic idea is that, with different implementations, common failure modes will probably cause different error effects. To the best of our knowledge, there is no metric for *measuring diversity* among designs with the same specification. However, the need for such a metric has been expressed in the literature [Tamir 84]. In addition to common-mode failures, it is interesting to find out whether design diversity also helps in achieving better compensating effects of different faults, compared to non-diverse systems.

2. Design Diversity Metric

Consider two implementations (N_1 and N_2) of the given combinational logic function with n inputs. Let V_i and V_j be the set of input combinations that detect fault f_i and f_j in N_1 and N_2, respectively. We define:

$$r_{i,j} = \frac{|V_i \cap V_j|}{2^n} \text{ and } q_{i,j} = 1 - \frac{|V_i \cap V_j|}{2^n}$$

The metric $r_{i,j}$ is the probability that a system having two copies of the same logic function produces an incorrect value at the system output when faults f_i and f_j affect the first module (N_1) and the second module (N_2), respectively. We performed reliability analysis using the q metric. Our reliability equation includes both the q metric and the mission time. Our calculation shows that system reliability is more strongly dependent on q for common-mode failures than for independent multiple module failures. For a given pair of q values, we quantified the improvement in reliability by calculating the ratio of the corresponding unreliabilities. In Fig. 2.1, we show how this improvement varies with mission time for a given pair of q values. On the Y-axis of the graph in Fig. 2.1, we plot the ratio of the following two quantities: (1) the unreliability with q = 0.9 at any time point i and (2) the unreliability with q = 0.99 at the same time point i. On the X-axis, we plot the mission time (normalized to the MTTF of a simplex system). As Fig. 2.1 shows, the ratio diminishes with longer mission times.

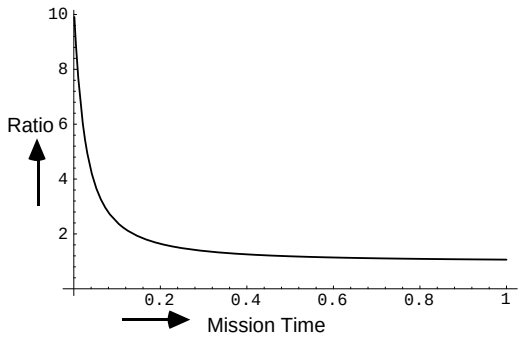

Figure 2.1. Effect of diversity with mission time (for CMFs)

For replicated systems, we can define a common-mode failure as one that produces identical faults (and hence, identical errors) in the two systems. However, for diverse copies, in the absence of information about the actual common-mode fault mechanisms and their effects in the circuit level, we resort to simulation by choosing random pairs of faults in an unbiased way. For simulation purposes we used the stuck-at fault model.

3. Simulation Results

It is very difficult to model the entire complex system mathematically even with the stuck-at fault model. Hence, in addition to mathematical models, we developed a simulation environment to examine the reliability of a redundant systems with and without diversity. We ran 100,000 simulations for each experiment so that our results are statistically significant. After performing all the simulations, we calculate the mean time to failure (MTTF) for the system. The improvement in the MTTF over the MTTF of a classical non-diverse system is an indicator of the effectiveness of using a diverse modules in the system.

For generating diverse designs, we minimized the given truth table using *espresso* and synthesized a logic circuit using *sis*. Next, we complemented the outputs in the given truth table to generate a new truth table and used the same synthesis procedure for this new truth table. Finally, we added inverters at the outputs of the new design obtained. These designs are referred to as T and C. We used some of the MCNC benchmarks for our simulations.

Our results show that *for independent failures in multiple modules, it is not necessarily true that diverse TMR implementations will survive (produce correct outputs) for a longer time compared to their non-diverse counterparts.* Table 3.1 shows results comparing the error latency of duplex systems with and without diversity and shows the relationship with the q-metric. *The results validate our theoretical result that the reliability of a redundant system is more closely related to the q metric rather than whether the copies are diverse or not.*

Table 3.1. Comparison of error latency in diverse and non-diverse duplicated systems

Circuit	Copies	Error Latency (cycles)	% fault pairs with $q = 1$
Z5xp1	T, T	6733	66.96
	T, C	6869	68.76
apex4	T, T	8594	85.71
	T, C	8094	80.51
clip	T, T	7951	79.24
	T, C	7869	78.44
inc	T, T	7666	76.54
	T, C	7516	75.08
	C, C	7512	74.90
rd84	T, T	7638	76.23
	T, C	6797	67.73

Table 3.2. Error latency in diverse and non-diverse system (common-mode faults)

Circuit	Copies	Error Latency
Z5xp1	T, T	15
	T, C	6869
apex4	T, T	106
	T, C	8094
clip	T, T	60
	T, C	7869
inc	T, T	12
	T, C	7516
	C, C	14
rd84	T, T	49
	T, C	6797
	C, C	24

In a duplicated system with identical copies, we can find a one-to-one correspondence between the leads of the two copies. Hence, for these systems we injected fault pairs (f_1, f_2) such that f_1 and f_2 affect lead *i* of Module 1 and Module 2, respectively. For diverse copies there is no such a one-to-one correspondence. Using the q metric, it can be shown that for a common-mode failure, the error latency in a diverse system is no worse than that in a non-diverse system. In order to estimate the gain (increase) in error latency using diversity, we performed 100,000 simulations — in each experiment we randomly chose a fault pair and calculated the error latency. Table 3.2 shows the average error latency we obtained from these simulations. *These results show a distinct advantage of using diverse implementations over non-diverse designs for common-mode faults.*

As shown in Table 3.3, *diversity is also useful for enhancing the self-testing property of redundant systems.*

Table 3.3. Self-testing properties of duplex systems

Circuit	Copies	% detected
Z5xp1	T, T	99.27
	C, C,	99.35
	T, C	99.98
inc	T, T	99.21
	C, C	99.16
	T, C	99.97
rd84	T, T	99.26
	C, C	98.90
	T, C	99.96

4. Summary

In this paper, we have addressed the issue of design diversity in redundant systems in order to handle common-mode failures and failures in multiple modules. For the first time, we have introduced a metric to quantify diversity among different designs under a particular fault-model, and performed the analysis of overall system reliability in terms of this metric. We have produced simulation results to model real-life environments that inject multiple failures. Our results show that, in the presence of independent multiple module failures, there is no obvious advantage of using diversity to increase the MTTF of a TMR system. On the other hand, for common-mode failures, there is a significant gain in the error latency (and hence MTTF) that can be achieved with diversity. But, the gain decreases with increasing mission time. However, there is further need to characterize common-mode failure mechanisms in the circuit level. Our results demonstrate that diversity plays an important role in enhancing the self-testing property of a system.

5. References

[Avizienis 77] Avizienis, A. and L. Chen, "On the implementation of N-version programming for software fault-tolerance during program execution," *Proc. First Intl. Computer Software and Applications Conference*, pp. 149-155, 1977.

[Avizienis 84] Avizienis, A. and J. P. J. Kelly, "Fault Tolerance by Design Diversity: Concepts and Experiments," *IEEE Computer*, pp. 67-80, August, 1984.

[Lala 94] Lala, J. H. and R. E. Harper, "Architectural principles for safety-critical real-time applications," *Proc. of the IEEE*, vol. 82, no. 1, pp. 25-40, January, 1994.

[Riter 95] Riter, R., "Modeling and Testing a Critical Fault-Tolerant Multi-Process System," *Proc. FTCS*, pp. 516-521, 1995.

[Tamir 84] Tamir, Y. and C. H. Sequin, "Reducing common mode failures in duplicate modules," *Proc. ICCD*, pp. 302-307, 1984.