TMR-Protection with Reduced Area Overhead Patent Application: DE 10 2010 006 383.5

I. Summary

In this patent application it is invented how the necessary area for a fault-tolerant Triple Modular Redundancy system (TMR) can be considerably reduced. The same high level of fault-tolerance as for TMR is guaranteed for a subset of safety critical inputs. This subset is specified by the designer. For the remaining inputs the system is not fault-tolerant. This approach is of special interest for safety-critical applications such as automotive, health-care, power plants, space and others. If the system is fault-tolerant for 30% of its inputs the necessary area can be reduced by about 100% compared to TMR.

II. Basic idea

In a TMR system a system S is triplicated into three identical systems. The outputs of the triplicated systems are connected to a majority voter V, as shown in Fig. 1a. If one of the triplicated systems is erroneous this error will be tolerated. The main disadvantage of TMR is its high area overhead of about 300% of the original system S. The invention allows considerably to reduce the area overhead by adapting the design to the real needs of fault-tolerance. According to the invention to the original system $S = S_1$ two smaller systems s_2 and s_3 are added. Their outputs are, as for TMR, connected to a majority voter. By the proposed design the behavior of S_1, s_2 and s_3 is identical for safety critical inputs, and under the safety critical inputs an arbitrary fault of one of the systems S_1, s_2 or s_3 will be tolerated at the output of the voter V. For every other input the system is not fault-tolerant. The smaller additional systems s_2 and s_3 provide good potential for optimization. First we create s_2 as follows:

$$s_2(x) = \begin{cases} S_1(x) & \text{if input is critical} \\ - & \text{don't-care otherwise} \end{cases} \quad (1)$$

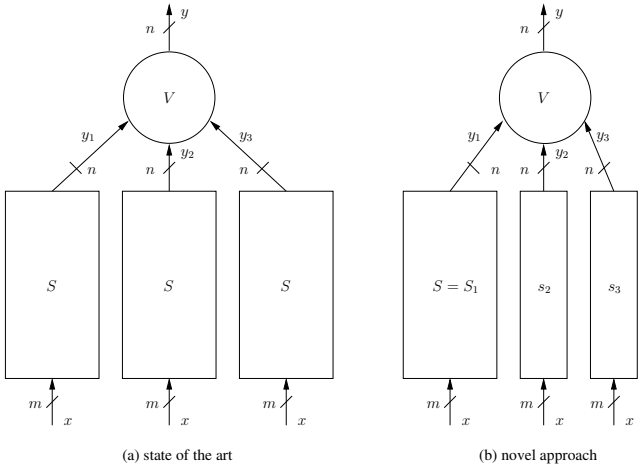
In the next step s_2 is optimized by a synthesis tool that takes advantage of all the don't care values of s_2. Now $s_3(x)$ is determined as:

$$s_3(x) = \begin{cases} S_1(x) & \text{if input is critical} \\ S_1(x) & \text{if } S_1(x) \neq s_2(x) \\ - & \text{don't-care otherwise.} \end{cases} \quad (2)$$

Again the partially defined Boolean function $s_3(x)$ is optimized. It is obvious that the optimization processes can only result in the original system in the worst case.

III. Experimental results

We implemented the invention on four LGSynth91 benchmark circuits with an input sample distance of 10%. The results are shown in figure 2. A size of 100% equates to a single system and 300% relates to a TMR approach. It can be seen that if we protect for example about 30% of all possible inputs, we can save the size of one complete system.



(a) state of the art (b) novel approach

Fig. 1. TMR vs. selective signal protection

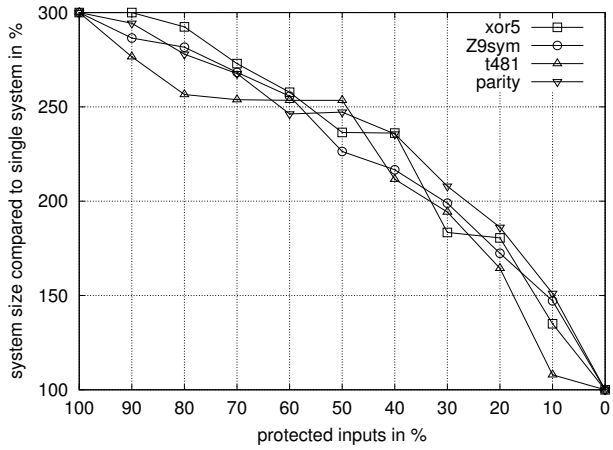


Fig. 2. Average area consumption per degradation step

IV. Contact

For further information just contact the authors via e-mail:
Michael Augustin (augustin@tu-cottbus.de)
Michael Gössel (mgoessel@cs.uni-potsdam.de)
Rolf Kraemer (kraemer@ihp-microelectronics.com)