

Faster, Better, Cheaper Space Flight Electronics - An Analytical Case Study

R. Katz

NASA Goddard Space Flight Center, Greenbelt, MD 20771

Abstract

The past decade has seen a major change in how projects are designed, developed, and built. "Faster, Better, Cheaper" has become and the standard mantra. On the technology side, for electronics, there has been a greater use of both commercial devices as well as commercial software, such as computer aided engineering systems. Programmatically, there have been additional changes as well, with NASA having a different role in the design and review of spaceflight electronics.

One such management experiment is "PI Mode," where the Principal Investigator takes full responsibility for a mission. The first of these programs provides a case study for this paper. We shall review the electronics design and provide analysis, showing the results of this program. Part of the philosophy is to use the contractor's design rules and for the contractor to review their own design. An analysis of the design rules will provide insight into the appropriateness of the developmental model.

The full paper will provide in-depth analysis of sample circuits and will be primarily a technical paper. This abstract will provide an overview; detailed circuits and analysis will be included in the full paper.

I. INTRODUCTION

This summary will provide an overview of the topics that will be addressed in the full paper. Details will also be addressed in the full paper.

Traditionally, for total dose measurement of microcircuits, radiation test protocols employed a step radiation procedure. That is, the devices under test (DUTs) would be tested, exposed, under bias, and then tested again. This cycle would be repeated until the DUTs received the required dose of radiation. No control or monitoring of the part was done in the chamber and the device was statically biased with power supplies.

While this step radiation method produces results, there are several shortcomings with this approach. First, it is extremely costly and labor intensive. Secondly, there is an aliasing problem since the devices responses inside of the chamber are not observed. This hurts test planning since it is difficult to determine when to end a test. Lastly, the lack of observations leads to a lack of understanding, including key hints as to the cause of

failure in the device and clues as to the underlying cause of the failure mechanisms.

II. DESIGN QUALITY

It was found that the logic design techniques and practices utilized in the electronics are in general not suitable for high-reliability space flight electronics and would normally be rejected at a design review. Circuits were found in the flight hardware that are textbook cases of logic design errors. The errors were not isolated but were prevalent throughout the design. Indeed, since the PI for this mission was at a university, it was initially thought this may have been a factor. However, course notes for the introductory logic design class clearly noted unsuitable circuits. Overall, the design is considered poor.

The logic errors fell into several categories. First, the technology was not well understood by the designers. This led to problems with the management of clock skew and power-on reset (POR) circuits, for example.

Knowledge of basic logic design was missing. This includes the use of counter's ripple carry out as both clocks and asynchronous clears and the designer did not realize that the circuits could glitch. Similarly, the design included multiple instances of decoders asynchronously decoding counts of synchronous counters. These decodes were used as clocks. Exacerbating the problem was that high levels of clock skew would add to the probability of glitches. One class of logic circuits, repeated in different places in the design, used circuit structures that had static hazards. Why were these errors made? It became apparent that the design engineer did not view the circuit as an electrical design but as a "logical design." Thus, a counter was viewed as sequencing from 01111 to 10000, permitting an asynchronous decoder to be used. Any experienced designer knows the risks of circuits of this class and it would never appear in a schematic.

The design planning was poor. For example, clock signals present on a global, low-skew clock were driven through local, high-skew buffers and then used for a clock. The concept of using signals as enables for a master clock was not employed. Since the clock signal was already on the global net, there was no power savings by then placing the signals on local nets. In many cases, global clock resources went unused, needlessly.

The designers were not familiar with standard logic structures that are tolerant of high skew on the clock signals (details and analysis will be presented in the full paper). Since the clock frequencies were low for the technologies employed, there was many techniques available that could produce reliable designs. These include the use of latches and two-phase non-overlapping or opposite edge clocking. The designers locked themselves into a box and did not explore any alternatives.

III. DESIGN RULES, QUALITY CONTROL AND VERIFICATION

A class of problems encountered was that the computer aided engineering (CAE) tools were not understood and properly utilized. The designers were unfamiliar with the static timing analysis and did not understand the limits of back-annotated logic simulation. Simulation and analysis concepts were not recognized as separate concepts and, consequently, the analysis was not properly performed. This, coupled with the designers not having a model of the actual hardware, led to incorrect results and poor circuits being accepted. The assumption inherent in most logic simulators, that all parameters track, is not valid for real circuits. The designers did not perform appropriate min-max analysis.

The contractor did have in place their own set of design rules. The analysis of this program showed their was two general flaws. First, conclusions about their design rules were not valid. Secondly, the design rules were not consistently followed. Indeed, it is apparent, that there was no effort at verifying either the design rules or whether they were followed. A few examples are given below. The full paper will have additional examples, detailed circuits, and a thorough analysis.

The designers routinely used local, high-skew signals in Actel FPGAs as clocks for parallel circuits. They felt that the circuits would work if they avoided long routing tracks and their logic design techniques, at the schematic level, would "guarantee" that long tracks were not used. Their analysis documents did not describe how this worked. Examinations of the flight database clearly showed that long tracks were used. The segmentation files were examined and will be presented as one of the specific cases. It is apparent that the output of the place and route algorithms were never examined. Sample outputs will be presented.

Their analysis guidelines relied on minimum delays. For example, they stated that the worst-case $t_{CLK \rightarrow Q}$ was 5.0 ns, minimum. Buffers were used between shift register "segments" to introduce skew in the desired direction and the "analysis" used 10.0 ns as the minimum t_{PD} . Unfortunately, it was trivial to show that these values were not even close to worst-case.

Using the static timing analysis, violations were found on the first circuit examined in just a few minutes. This indicates that there was no serious review or verification of the design or design rules.

Independent of the quality of the rules, it is critical that a rule set be strictly enforced. Like above, it was trivial to find areas where the contractor's rules were violated. For example, local clock signals were supposed to be arranged in a "reverse buffered" topology, where downstream flip-flops were clocked before upstream flip-flops. This was in place for a lot of the circuits. Multiple circuits were found that had a clock tree topology, with unfavorable skew characteristics. Four different versions of one standard interface module, two in violation of the contractor's rules, were found. One circuit had the "reverse buffering" topology incorrectly implemented with skew being introduced in a direction that was most unfavorable. Again, it was clear that this program had no serious or even casual review or effort at verification.

For critical signals, fanout control was used to help manage skew, with 5 set as the upper limit for critical structure. The contractor's rules were violated multiple times, with one instance of 23 loads found. Because of the hierarchical structure of the design, the load was not apparent without a bit of looking. Additionally, the information was available at the output of the Combiner but the report was not examined.

Other examples will be given in the full paper.

IV. CONCLUSION

It is felt that reliable electronics can be built "faster, better, and cheaper" if it is properly managed and if competent, experienced engineers are used. While it is tempting to speed up development and cut costs by eliminating thorough reviews, it is found that that is often a false economy, particularly with an inexperienced design team. Indeed, the output automatically produced by the tools was not even examined. The use of modern technology is not a replacement for understanding. We have seen, in the program used for our case study, a lack of basic knowledge of circuit design and analysis, the microcircuit technology, and design tools such as logic simulators and static timing analyzers. Poor design planning was evident, for which there is no good excuse. The structures supplied by the microcircuit vendors, both low-skew resources and flip-flops with enables that make their use rather straightforward, were not used. Standard solutions to common problems for clock skew, available at the logic design level, were not explored. Faster, better, and cheaper are all obtainable. Technology, however, is not the answer. Experience, knowledge, and analysis is.