Mitigating Soft Errors to Prevent a Hard Threat to Dependable Computing

Yves Crouzet, Jacques Collet, Jean Arlat
LAAS-CNRS, 7, Av. Colonel Roche, 31400, Toulouse (France)
{crouzet, collet, arlat}@laas.fr

Abstract

This paper presents first the context and motivation for dealing with soft errors. In order to be able to account for the various issues involved, a concerted reflection has been carried out including embedded system integrators, manufacturers, and academic researchers. We summarize the main outcomes of this effort. Finally, we introduce the various contributions that are meant to address the several factors that characterize the problem posed by soft errors and provide solutions to mitigate their effects.

1. Context and motivation

Equipment suppliers in various application fields must cope, to grant their customers' request, with the permanent and increasing complexity of applications, which results in more and more embarked computing power.

On one end, this evolution suggests selecting modern processors, or at least processors featuring the latest technological developments, so as to support ever more complex and performance-demanding functionalities.

On the other end, due to the reduction in size of the elementary devices and in the energy associated to the information bits, new technologies are decreasing their natural resilience to **soft errors** induced by radiation effects (alpha particle, cosmic rays, as well as thermal neutrons) [1]. A *soft error* is the resulting effect of a transient fault where only data are lost (e.g., a bit-flip). Although no damage affects the internal structure of the semiconductor, such errors are nevertheless prone to lead to malfunctions and even failures of the circuit.

As a matter fact, such a problem, which is well-known for years in space applications, is now concerning a wider range of application domains. Of course, one can think of embedded avionics systems, but ground-based applications can be impacted as well.

A comprehensive set of tests carried out by IBM at various terrestrial altitudes — high (10,000 ft), moderate (5000 ft), sea level, revealed that all elevated-altitude tests showed cosmic-ray-induced fails in electronic components [2]. Another example concerns the malfunction reported in 1999 of Sun Microsystems routers that were traced to soft errors affecting SRAM components.

Recently, problems were reported showing that the impact of soft errors was not limited to memory components, but was perceived in other digital components, including not only SRAM-based FPGAs [3], but combinational logic [4]. The high frequency of operation of modern ICs has a major impact on this trend. This means also an increased impact on microprocessors behaviors in addition to consequences attached to storage devices.

More importantly, irrespective of the cause — e.g., single event upset (SEU), single event latch-up (SEL), single event transient (SET) — and of the magnitude of the soft error rate (SER), experts agree that the vulnerability of digital circuits will keep increasing in the near future.

After the risks and threats had been recognized, semiconductor manufacturers, aerospace system integrators, related government agencies and academic research groups have started independent research programs to cope with several facets of the problem.

Within the framework of RIS - *Réseau d'Ingénierie de la sûreté de fonctionnement* (Network for Dependability Engineering), LAAS-CNRS has initiated a working group to deal with these issues in a comprehensive way. Indeed, the group has gathered various key players encompassing embedded systems integrators (Airbus, Astrium, Thales Avionics and Technicatome), space agencies (CNES and ESA) and academic partners (TIMA, and LAAS).

This session summarizes the results of the reflection carried out in this framework. In the next section, we briefly present the main issues that were identified.

2. How to mitigate these threats?

In this context, it is not always clear what kind of decision should be made concerning the kind of processor to be integrated and more specifically, which approach should be adopted to deal with the soft error

Proceedings of the 11th IEEE International On-Line Testing Symposium (IOLTS'05)
1530-1591/05 $20.00 © 2005 **IEEE**

issues: "hardening" at the component level or "hardening" at the level of the architecture of the system?

In order to address these two alternatives one need to consider several factors:

1) Assess the gap in performance between the computing power offered by the components complying with each alternative.
2) Characterize the environment in which the target computing system will operate.
3) Identify the requirements attached to the industrial domains. Due to the effects to be considered, emphasis is to be put on aerospace domain. However, it is anticipated that the automotive industry should be concerned as well. Indeed, this is pushed up by the so-called "X-by-wire" trend in which, functions usually implemented as mechanical and hydraulic mechanisms are increasingly replaced by distributed computerized entities. This concern about soft errors has been explicitly recognized in [5].
4) Account for the location and role of the target component into the computing system. Actually, distinct alternatives may apply to components of a same system. Indeed, for peripheral functions (e.g., DSPs) component hardening might be preferred, because hardening at the architectural level is usually cumbersome and for exploiting existing hardened FPGA components. However, for basic processing resources, it might be decided to use standard COTS components instead, in order to reach a sufficient computing power and because it might well be the case that redundancy schemes are already used to cope with permanent faults.
5) Select cost-effective component hardening techniques. The associated overhead in device size, clock frequency should be carefully assessed.
6) Identify the suitable redundancy technique. Even in the case when the architectural hardening option is considered, it is necessary to carefully analyze the possible alternatives among the various fault tolerance mechanisms [6].
7) Assess the dependability of solutions being developed. This is mandatory irrespective of the chosen alternatives. It is necessary to be able to study the detailed impact of SEUs into complex components and systems. This requires that multilevel descriptions be considered to be able to propose cost-effective solutions.
8) Plan further research and development programs to support the emergence of approaches to i) better characterize the risks and impacts of soft errors and ii) to define and implement cost-effective solutions to cope with these issues. For example, a set of relevant and comprehensive guidelines covering a large spectrum of application domains (airborne, space, automotive, nuclear, defense, medical), as well as selected US-government-supported initiatives concerning electronics COTS hardware components, can be found in [7].

Except for item 1) above, all these issues are addressed by the other contributions of the session. Accordingly, before outlining these various contributions, in the sequel, we present first a brief discussion on the trend in processor technology. The subsequent section, will introduce the successive contributions.

3. Trend in microprocessor technology and dependability issues

When deciding to select a processor to be integrated into a critical embedded system, several options can be considered. One may consider to embark a recent superscalar processor (Pentium IV, Athlon 64 or Power PC) featuring the 80 nm technology that operates in the 3-4 GHz range and whose computing power reaches 10^4 millions of instructions per second (MIPS). Figure 1 describes the evolution of modern processors with respect to computing power and clock frequency.

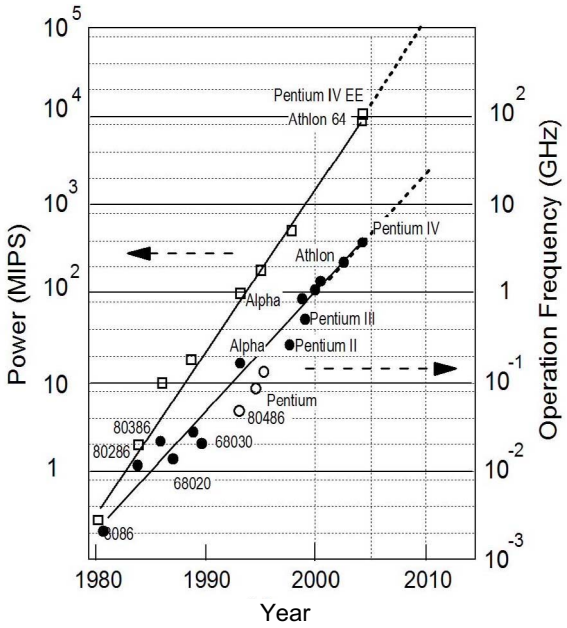

Figure 1: Evolution of the processing power and operation frequency of processors

The rapidly changing technologies of the commercial sector, coupled with the virtual disappearance of suppliers for radiation-hardened components, lead to significant challenges.

From the point of view of cost, COTS processors are very attractive, but their development is primarily targeting non-critical applications (such as desktop computers, games, etc.). Thus, they are not well suited for harsh environments in which critical embedded systems are operating (especially aerospace applications).

Accordingly, the primary question is how to be able to ensure dependable computing in spite of soft errors that may affect COTS processors? It is needed that its sensitivity to radiations be carefully analyzed. This means the SER be assessed with respect to the considered radiating environment (altitude and latitude) and to various effects induced (SEU, SET, SEL, etc.) that are described and discussed in the various contributions to this session. What kind of measurements are necessary and what evaluation techniques can be applied to estimate a realistic SER? How to exploit this information to define the fault tolerance mechanisms suitable to cope with the ineluctable faults that will affect the operation of the processor?

Conversely to the COTS-based alternative, the alternative previously discussed concerns the design and implementation of advanced processor architectures that are either virtually immune to the effects of cosmic rays (e.g., the Lookheed Martin's Power PC 750) or can tolerate them (e.g., ESA's LEON2 SPARC V8-based fault-tolerant processor [8]. The related questions are: What are the most suitable hardening techniques? At what level should hardening be applied in the physical structure (transistor, component)? How to protect the high-speed communication links and the associated protocols?

Moreover, the choice of hardened components results in a significant reduction in processing power with respect to most recent COTS. Indeed, while a standard Power PC 750 processor delivers a computing power of about 300 MIPS (assuming a 133 MHz clock frequency) a LEON2 processor would be only about 120 MIPS (assuming a 140 MHz clock frequency). Alternatively, when processing power is not mandatory one can consider radiation hardened FPGA components (Actel, Xilinx) that integrate about 2 million of gates.

Finally, it is worth noting that the application of fault tolerance techniques is facilitated by the very specific (soft) nature of the errors induced by most radiation effects. Indeed, focus can be concentrated on the numerous error detection and recovery mechanisms suitable for handling transient faults (e.g., see [6]).

4. Session outline

As previously indicated, the selected contributions that are reported hereafter are made by participants to the RIS working group. The aim at providing insights on the issues listed in Section 2.

The first contribution sets up the scene by introducing the problem and discussing the difficulties that computer system suppliers face in the space (Astrium) and avionics (Thales) domains. Indeed, these two application domains are definitely the most impacted by soft errors.

The two subsequent contributions report on relevant research activities. They show how to characterize the problem and how it is possible to analyze the possible impacts of SEUs either at component level or at system level.

The second contribution, by TIMA and CNES, first summarizes representative examples of anomalies observed for systems operating on-board satellites as the consequence of the effects of radiations affecting integrated circuits. It also briefly describe an approach suitable to predict the sensitivity to SEUs of processor-based architectures.

The third contribution is by TIMA researchers and reviews the main approaches used to evaluate the impact of SET and SEU effects in digital circuits that are described at different abstraction levels. The two fault models are first discussed with respect to the circuit description levels, then complementary dependability evaluation methods are summarized.

The next two contributions review the main solutions that are currently considered at the component and system levels, respectively.

The fourth contribution, by Atmel Inc., illustrates on a family of processors the application of hardening solutions at chip level.

Alternatively, contribution number five, from CNES, describes various schemes that can be planned at system level when considering to include standard COTS components, thus requiring the development of customized fault-tolerant architectures.

Finally, the sixth contribution summarizes the initiatives of a space agency, such as ESA, to lead the efforts in research and development towards solutions adapted to the mitigation of soft errors.

Acknowledgement

This paper and to a large extent the subsequent contributions to this session report on reflections carried out in the framework of the topical working group set up by RIS (Network for Dependability Engineering)[1] to investigate the impact of technology trend with respect to soft errors and dependability issues. The authors would like to thank all the participants to the working group, and in particular the contributors to this session. The support received from the organizers of the 2005 edition of the IEEE International On-Line Testing Symposium is also gratefully acknowledged.

References

[1] T. Karnik, P. Hazucha and J. Patel, "Characterization of Soft Errors Caused by Single Event Upsets in CMOS Processes", *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 2, pp. 128-143, April-June 2004.

[2] J. F. Ziegler, H. W. Curtis, H. P. Muhlfeld, C. J. Montrose, B. Chin, M. Nicewicz, C. A. Russell, W. Y. Wang, L. B. Freeman, P. Hosier, L. E. LaFave, J. L. Walsh, J. M. Orro, G. J. Unger, J. M. Ross, T. J. O'Gorman, B. Messina, T. D. Sullivan, A. J. Sykes, H. Yourke, T. A. Enger, V. Tolat, T. S. Scott, A. H. Taber, R. J. Sussman, W. A. Klein and C. W. Wahaus, "IBM Experiments in Soft Fails in Computer Electronics (1978-1994)," *IBM J. Research and Development*, vol. 40, no. 1, pp. 3-18, January 1996.

[3] R. Mariani, "Soft Errors on Digital Components", in Chapter 1.3 of *Fault Injection Techniques and Tools for Embedded Systems Reliability*, Kluwer Academic Publishers, (A. Benso, P. Prinetto, Eds.), ISBN 1-4020-7589-8, pp. 49-60, 2003.

[4] P. Shivakumar, M. Kistler, S. W. Keckler, D. Burger and L. Alvisi, "Modeling the Effect of Technology Trends on the Soft Error Rate of Combinatorial Logic," *Proc. IEEE/IFIP Int. Conf. On Dependable Systems and Networks (DSN-2002),* Washington, DC, USA, pp. 389-398, (IEEE CS Press), 2002,

[5] M. Baleani, A. Ferrari, L. Mangeruca, A. Sangiovanni-Vincentelli, M. Peri and S. Pezzini, "Fault-Tolerant Platforms for Automotive Safety-Critical Applications," *Proc. ACM/IEEE Int. Conf. on Compilers, Architectures and Synthesis of Embedded Systems (CASES-03),* San Jose, CA, USA, pp. 170-177, (ACM Press), 2003.

[6] J. Arlat, Y. Crouzet, P. David, J.-L. Dega, Y. Deswarte, J.-C. Laprie, D. Powell, C. Rabéjac, H. Schindler and J.-F. Soucailles, "Fault Tolerant Computing," in *Encyclopedia of Electrical and Electronics Engineering,* (J. G. Webster, Ed.) vol. 7, pp. 285-313, New York, USA: J. Wiley & Sons, 1999.

[7] Review of Pending Guidance and Industry Findings on Commercial Off-The-Shelf (COTS) Electronics in Airborne Systems, Tech. Report DOT/FAA/AR-01/41, National Technical Information Service (NTIS), Springfield, VA, 125 p., USA, 2001.

[8] J. Gaisler, "A Portable and Fault-Tolerant Microprocessor based on SPARC V8 Architecture," *Proc. IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN-2002),* Washington, DC, USA, pp. 409-415, (IEEE CS Press), 2002.

[1] See http://www.ris.prd.fr for more detailed information on RIS activities.