Diagnostic and Error Correction System for Avionics Devices in Presence of Single Event Upset (SEU)

Marcantonio Catelani, Lorenzo Ciani

Department of Information Engineering, University of Florence, via S.Marta 3, Florence (Italy)

Abstract- In aerospace applications, Commercial-Off-The-Shelf (COTS) Field programmable Gate Array (FPGA) is becoming increasingly attractive by offering low-cost solutions, simplicity and flexibility.

This research faces the problem of disturbance induced by high energy particles on electronic devices. Based on detailed analysis of this phenomenon, the work is divided into two parts: in the first part evaluation of effects of the Single Event Upset (SEU) has been carried out with the aim of determining diagnostic techniques and the mitigation of this disturbance, taking into account the fact that testing is one of the fundamental points in electronic programmable devices; in the second part a fault tolerant technique has been devised so as to achieve the requirements demanded on a real avionic system. For this purpose, a model of calculation to establish whether the system respond to specific requirements has been developed.

I. Diagnostic and mitigation techniques for radiation phenomena

The techniques for diagnosis and mitigation are classified in fault avoidance and fault tolerant techniques [1-3]. The first one consists in hardware techniques that allow to reduce the sensitivity of the device to radiation, that is, reduce the probability that upset will occur.

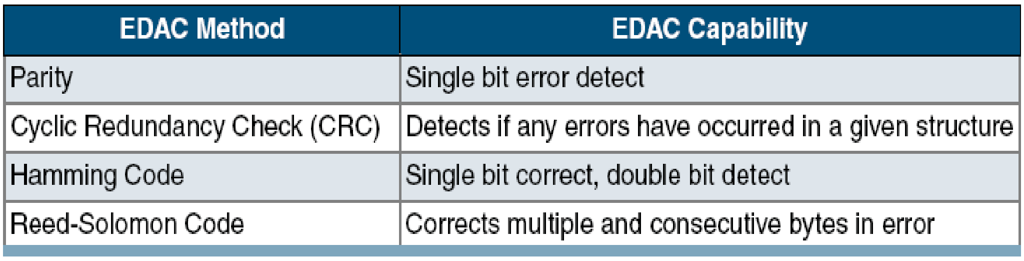
A large number of design solution have been developed for memory cells, latches, and registers; in particular, such solutions aim to reduce the bandwidth of the cell to achieve immunity to the transient caused by collected charge or to provide redundant storage or blocking provision to prevent upset.

Although effective in improving cell single event upset characteristics, the disadvantages of hardening the process are that the cost and the die size might increase and the performance of the device is typically reduced. Moreover the reduced bandwidth is contrary to the achievement of high-speed operation.

Fault tolerant techniques, instead, allows the system to function even in the case of fault. These techniques use redundancy to disguise, correct or reveal eventual upset and are the same ones used to protect digital system from any other type of error. Implementation of fault tolerant typically utilizes some form of redundancy; variations include informational redundancy (redundant data structures), spatial redundancy (redundant hardware), and temporal redundancy (redundant sequential operations).

The most common way of mitigating SEUs in semiconductor devices is by error detection and correction (EDAC). Today, a large number of designs incorporate some form of EDAC. Some common methods of EDAC are shown in Table I [4].

Table I. EDAC methods.



EDAC Method	EDAC Capability
Parity	Single bit error detect
Cyclic Redundancy Check (CRC)	Detects if any errors have occurred in a given structure
Hamming Code	Single bit correct, double bit detect
Reed-Solomon Code	Corrects multiple and consecutive bytes in error

The increase in hardware content in informational redundancy is typically less than spatial modular redundancy. Informational redundancy consists in the addition of k bit of control to the m bit of information, so obtaining coding from m+k bit. This coding lets us have 2m+k combinations, 2m will single out valid words, the others will make up words which are not valid so that the Hamming distance of the coding is greater than zero. We refer to the fact that the distance of Hamming is defined as the number of bit for which two valid words differ. It also known that if the minimum Hamming distance of the coding is equal to t+1, t errors can be revealed, whereas it must be at least equal to 2t+1 to correct t errors.

Fault tolerant techniques which are more suitable for this kind of disturbance, have been studied [5-6]:

- Parity bit technique needs the addition of only one control bit to make the number of "1" of the word equal. This technique allows an odd number of errors to be revealed but doesn't allow them to be corrected.
- Single Error Correction – Double Error Detection (SEC-DED) allows the correction of single errors and reveal multiple upset on two bit. As the SEU is an effect which interests the upset of a bit and MBU strikes mainly two bit, the SEC-DED technique is particularly adapt for this type of disturbance.
- Cyclic Redundancy Check (CRC) only lets errors be revealed. Its performances depend on the algorithm which determines number and form of the control bit.
- Triple Modular Redundancy (TMR) a fault in an individual module is corrected by the action of a voter through the majority consensus, or two-out-of-three, voting rules.

Disturbance produced by high energy particles on an electronic device can result, in some applications, unacceptable. This is the case for avionics and space applications where project requirements demand high reliability levels and what's more, the extent of the disturbance is such that it can not be ignored.

For this work informational redundancy has been chosen in order to avoid an excessive use of hardware redundancies that often involve too much resources, a complex implementation neither integration with other diagnostic techniques present in the system.

However there are under consideration other employs of TMR technique in the avionics electronic subsystems presents as, for example, on the data acquisition channels from sensors [7]. In this work is described a general purpose high reliable data acquisition system which allows A/D converter testing by histogram and two tone tests for the fault diagnosis on the same board.

II. Proposed approach

In order to prove the validity of the proposed technique we can considered an avionic application. In particular, the aeronautics operating system under examination is an Integrated Control Panel (ICP) for military aircraft cockpit. The main task of system is to define the altitude of the airport for landing by means of an encoder, to visualize the selected value on a display and to transmit such information to the other systems constituting present in the aircraft cockpit. The block diagram of the integrated control panel in shown in Figure 3.

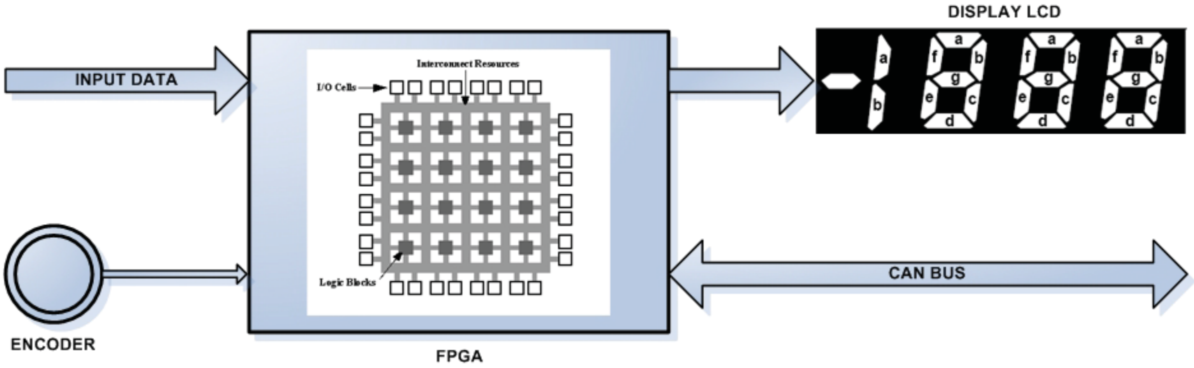


Figure 3. Integrated Control Panel (ICP) block diagram.

The device has a fundamental role in the management of the interface between the cockpit and other control systems of the airplane like the ILS, Instrument Landing System, and the ISS, Integrated Surveillance System, a system which analyzes the air and ground traffic, arranged with the weather radar and the transponder.

The functions of the system are carried out through a logic device realized with an FPGA. Such component receives signals from the encoder and translates them into information that are visualized on the display via I2C bus (Inter-Integrated Circuit) and, at the same time, send to the other subsystems of the cockpit by CAN bus (Controller Area Network bus).

For this operating system the FPGA represents the element subjected to the upset phenomenon.

Once the critical component of the surveillance display is located in the FPGA[8-11], it is necessary to do a detailed examination of the disturbances brought on by the high energy particles on this particular component. In literature [12] errors in FPGA are classified as:

- Permanent Errors – if the configuration memory is involved; permanent errors are considered as the worst type of errors and can be removed only with a new configuration of the memory. It is important to observe that these errors differ from those which damage the device (hard errors or physical defects). In this case, the configuration bit remains erroneous until the new configuration is downloaded into the FPGA. So, these permanent errors are recoverable.
- Transient Errors – they are errors localized in the combinational logic components, in the registers and in the user memory. These errors are called transient because they maybe overwritten or corrected using error-detection-and-correction techniques.

In Table II the upset rate value for the configuration memory, the user memory and the registers implemented in this project are evaluated. The values are obtained by tests carried out at the Los Alamos Laboratory (New Mexico, USA) [13], and relate to airborne environment by means of the Boeing model [14].

Table II. FPGA upset rates.

Altera FPGA – CyclonII (SRAM 90 *nm*)		
Configuration Memory **upset rate**	**Registers** **upset rate**	**User Memory** **upset rate**
$\lambda_{C\text{-}RAM}= 1.08\times10^{-4}\ n^{\circ}upset/(chip\cdot h)$	$\lambda_{reg}=1.6\times10^{-6}\ n^{\circ}upset/(chip\cdot h)$	$\lambda_{mem}= 2.39\times10^{-5}\ n^{\circ}upset/(chip\cdot h)$

We can observe how the configuration memory presents the biggest rate, because the cells are realized in SRAM technology which offers a high level of sensitivity towards this disturbance.

We choose informational redundancy techniques in order to avoid an excessive use of hardware redundancy which often lead to a loss of resources; by doing so we enabled a remarkable cost reduction and a significant increase of the resources available and of the systems' speed.

By means of a detailed risk analysis and assessment and of the reliability analysis of the possible design options, the best techniques have been chosen in order to comply with the project requirements. This assessment has been developed according to DO-178B [15], for the system software development, and DO-254 [16] standard, for the system hardware development. In this two standard have been indicated that avionics equipment contains both hardware and software, and each is critical to safe operation of aircraft.

The DO-178B (Software Considerations in Airborne Systems and Equipment Certification) is a guidance for software development published by RTCA, Radio Technical Commission for Aeronautics, that is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public.

The DO-254 (Design Assurance Guidance for Airborne Electronic Hardware) is a standard for complex electronic hardware development standard. Complex electronic hardware includes devices like Field Programmable Gate Arrays (FPGAs), Programmable Logic Devices (PLDs), and Application Specific Integrated Circuits (ASICs). The DO-254 standard is the counterpart to the well-established software standard DO-178B. European and American aviation administration accept use of DO-178B and 254 as a means of compliance for the design of complex software and hardware in airborne systems.

This risk analysis enables to achieve the system possible states and the reliability performances which it has to comply to, such as probability of occurrence of faults (Table III).

Table III. System States.

System State	**On**	**Loss**	**Erroneous**
Faults description	The system is working, there aren't errors or they are correct	It has been revealed the presence of errors in the system	The system is in a fault state, there are errors not detected or not corrected
Risk Classification	*No Effects*	*Major*	*Catastrophic*
Probability of Occurrence	10^{-3} per flight hour	10^{-5} per flight hour	10^{-9} per flight hour

The required probability of occurrence is determined from the risk assessment process and hazard analysis by examining the effects of a failure condition in the system. The failure conditions are categorized by their effects on the aircraft, crew, and passengers.

In table III with No effects is classified a condition in which a fault has no impact on safety, aircraft operation, or crew workload. The level Major means a significant reduction in aircraft operating margins with a reduction in the ability of the flight crew to cope with adverse conditions as a result of increase in workload or as a result of conditions impairing their efficiency and injury to occupants. Finally with Catastrophic is defined a failure condition that involve the possible loss of the aircraft and multiple fatalities.

Therefore, SEC-DED fault tolerant technique is introduced differentiating between harmful and unharmful errors and that is only data which lead to a variation of the permanent function have been protected, so reducing the complexity of the additional code: sign of the condition of state machine and data contained in the ROM (Read-only memory) implemented in the system.

A development of the SEC-DED technique has been realized for the state machine, the SEC-DED system together with the parity bit method has been used so allowing protection of the registers with SEC-DED code from eventual upset and the signal inside the logic, from eventual transition by means of parity bit. This is obtained by adding parity bit to the coding and by inserting the SEC-DED code onto the word. In this case it is necessary to implement a SEC-DED decoder inside the FPGA.

In Figure 4 is shown the state machine fault tolerant technique block diagram, where state is the state value register and output is the output value register.

The next state and output of this state machine is a function of the input and of the current state by means of combinational logic components indicated as CL – OUTPUT (for the output) and CL – STATE (for the state).

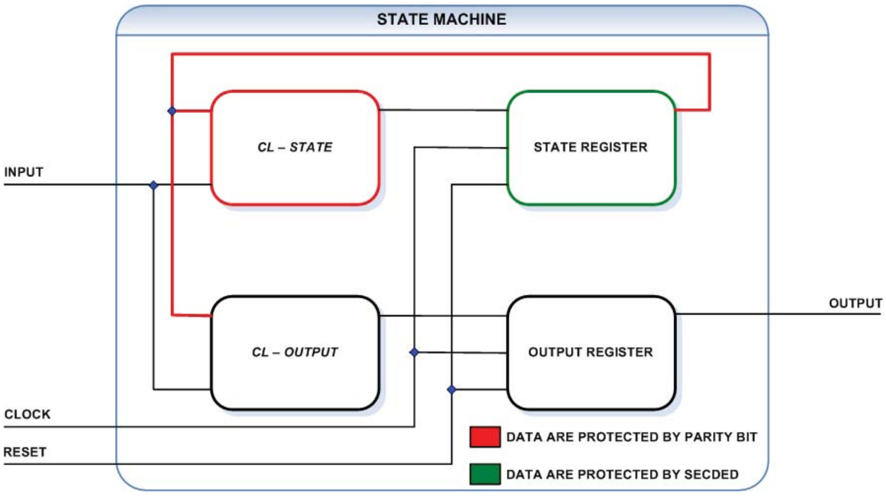


Figure 4. Block diagram of the State Machine fault tolerant technique.

The user memory is protected by directly storing data with the SEC-DED code and by checking the correctness which comes out with a SEC-DED decoder.

III. Conclusions

This research work has allowed us to understand breakdown mechanism brought about by high energy particles and to individuate in the neutrons, the predominant component of radiation in avionics and a mitigation technique for SRAM based FPGA avionics device has been proposed.

Acquired knowledge has allowed us to individuate diagnostic techniques and the mitigation of this disturbance and a reliability math model has been developed to estimate both the need to introduce fault tolerant techniques and which of these allow us to comply with the project requirements. Therefore a fault tolerant technique for a system present on a military aircraft has been analyzed and devised. The technique which has been developed is general purpose and can be introduced into any generic electronic device on an aircraft.

Electronics systems reliability problems, due to radiation disturbance, are also affecting other application fields (automotive, railway, biomedical) other than aerospace one. The achieved know-how and the diagnosis and mitigation techniques which have been carried out can be used in other critical applications connected to radiations phenomena. Furthermore the proposed technique represents an interesting solution also to guarantee the functional safety requirements [17-22].

References

[1] W. Heidergott, “SEU Tolerant Device, Circuit and Processor Design”, Proc. of the 42nd Annual ACM IEEE Design Automation Conference, Anaheim, CA, USA, 13 - 17 June 2005.

[2] Cary R. Spitzer, *Avionics Handbook*, CRC Press LLC, 2001.

[3] U.S.A. Department of Defense, *Military Handbook 338B – Electronic Reliability Design Handbook*, 1998.

[4] M. Kochar, K. Murchek, *Single event upsets in FPGAs*, Quicklogic Corporation, 2003.

[5] L. Ciani, M. Catelani, L. Veltroni, “Fault tolerant techniques to diagnose and mitigate Single Event Upset (SEU) effects on electronic programmable devices”, Proc. Of 16th IMEKO TC4 Symposium on Exploring New Frontiers of Instrumentation and Methods for Electrical and Electronic Measurements, Florence, Italy, Sept. 2008, pp. 794-798.

[6] L. Ciani, M. Catelani, L. Veltroni, "Single Event Upset (Seu): Diagnostic And Error Correction System For Avionics Device", Proc. of XIX IMEKO World Congress Fundamental and Applied Metrology, September 6-11, 2009, Lisbon, Portugal, pp. 1380-1384.

[7] L. Ciani, M. Catelani, G. Iuculano “Fault Diagnosis on Board for Analog to Digital Converters”, Proc. of IEEE Instrumentation and Measurement Technology Conference”, Warsaw, Poland, May 1-3 2007.

[8] Single-Event Effects in FPGAs, Actel, 2005

[9] P. Graham, “Consequences and Categories of SRAM FPGA Configuration SEUs”, Proc. of Military and Aerospace Programmable Logic Devices International Conference, Washington D.C., September 9-11, 2003.

[10] M. Sonza Reorda, L. Sterpone, M. Violante, “Efficient Estimation of SEU effects in SRAM-based FPGAs”, Proc. of 11th IEEE On-Line Testing Symposium, Saint Raphael, French Riviera, France, July 6-8, 2005.

[11] M. Caffrey, P. Graham, E. Johnson, M. Wirthlin, “Single-Event Upsets in SRAM FPGAs”, Proc. of Military and Aerospace Programmable Logic Devices International Conference, Laurel MD – USA, September 10-12, 2002.

[12] G. Asadi, M. B. Tahoori, “Soft Error Rate Estimation and Mitigation for SRAM Based FPGAs”, Proc. of 13th international symposium on Field-programmable gate arrays, Monterey, CA – USA, February 20 - 22, 2005.

[13] *Overview of iROC Technologies Report: radiation results of the test of FPGA december 2005*, Actel, Aug. 2006.

[14] E. Normand, “Single-Event Effects in Avionics”, IEEE Transaction on Nuclear Science, Volume 43, Issue 2, Part 1, April 1996.

[15] RTCA - Radio Technical Commission for Aeronautics, DO-178B/ED-12B, Software Considerations in Airborne Systems and Equipment Certification, 1999.

[16] RTCA - Radio Technical Commission for Aeronautics, DO-254, Design Assurance Guidance for Airborne Electronic Hardware, 2000.

[17] M. Catelani, L. Ciani, V. Luongo, "Safety Analysis in Oil &Gas Industry in compliance with Standards IEC61508 and IEC61511: Methods and Applications" Proc. Of IEEE - International Instrumentation And Measurement Technology Conference (I2MTC) - Minneapolis (USA) - May 2013, pp. 686-690.

[18] M. Catelani, L. Ciani, V. Luongo, "Functional safety assessment: an issue for technical diagnostics", Proc. Of XX IMEKO World Congress - Metrology for Green Growth, Sep. 9 - 14, 2012, Busan, Rep. of Korea

[19] M. Catelani, L. Ciani, V. Luongo, "A new proposal for the analysis of Safety Instrumented Systems" Proc. Of IEEE - International Instrumentation And Measurement Technology Conference (I2MTC) - Graz (Austria) - May 2012, pp. 1612-1616.

[20] M. Catelani, L. Ciani, V. Luongo, "A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application", Microelectronics Reliability, Volume 51, Issues 9-11, September-November 2011, Pages 1503-1507, ISSN 0026-2714, 10.1016/j.microrel.2011.07.044.

[21] M. Catelani, L. Ciani, V. Luongo, "The FMEDA approach to improve the safety assessment according to the IEC61508", Microelectronics Reliability, Issue 50, Vol. 9-11 (2010), pp. 1230-1235, ISSN: 00262714, DOI: 10.1016/j.microrel.2010.07.121.

[22] M. Catelani, L. Ciani, V. Luongo, R. Singuaroli, "Evaluation of the Safe Failure Fraction for an electromechanical complex system: remarks about the standard IEC61508", Proc. Of I2MTC 2010 (IEEE - International Instrumentation And Measurement Technology Conference) - Austin (USA) - May 2010, pp. 949-953.