International Journal of Hybrid Information Technology
Vol.7, No.5 (2014), pp.191-200
http://dx.doi.org/10.14257/ijhit.2014.7.5.18

SEU Mitigation for SRAM Based on Dual Redundancy Check Method

Peng Wang[1], Chengxiang Jiang[2], Zhen Li[2], Qiannan Xue[1*] and Yi Tian[1]

[1]*Tianjin Key Laboratory for Civil Aircraft Airworthiness and Maintenance, Civil Aviation University of China, Tianjin 300300, China;*
[2]*College of Safety Science & Engineering, Civil Aviation University of China, Tianjin 300300, China*
**Corresponding author (E-mail:qiannanxue@163.com)*

Abstract

The application of Static Random-Access Memory (SRAM), becomes more and more widely in aviation. However, the large amount of SRAM cells is very vulnerable to radiation included single-event upset (SEU). Based on the detection requirement of SRAM's SEU, the detected circuit of the SEU on SRAM is designed. Then the method of redundancy check is used in the reinforcement of the SEU. The test results shows that the detection circuit can detect the SRAM-type storage chip sensitive bit of the single particle and the proposed method can improved the performance of anti-single particles of SRAM several times as high as 1E6.

Keywords: *Mitigation; Fault Detection; Single Event Upset (SEU); SRAM; Cyclic Redundancy Check (CRC)*

1. Introduction

During the flight of the aircraft, the complex and changeable external environmental factors can cause a certain degree of impact on the airborne electronic equipment, seriously affecting the performance of aircraft flight. Because of the devices based on SRAM having high-density, low-cost, reconfiguration and other major advantages, they are becoming more and more popular in the field of aviation. However, the devices based on SRAM are more susceptible to single event effects (SEE), bringing serious security issues to aviation applications. The reinforcement methods have been studied, and they have made great progress in the triple modular redundancy [1-3], the refresh [4, 5], modified Hamming code [6, 7], and so on. Due to various reasons such as technology blockade, the research in this aspect is still in an exploring stage. Especially the research related with SEU in aviation is quite few. So in view of the SEU of the device based on SRAM, the studying of the strengthening design to improve the performance of the anti-SEU of devices based on SRAM becomes more important.

SEE is the event that high energy particles bombard sensitive nodes of microelectronic device, leading to the flip of the logic functions of microelectronic device or the damage of the devices. Depending on the mechanism of the different effect, SEE can be divided into the SEU [8, 9], single event latch-up [10, 11], single event function interrupt [12], and other types [13, 14]. Among them, the SEU is a charged radiation effect that occurs in monostable or bistable logic devices and logic circuit [15]. Its main phenomenon is that high energy particles in spatial have collision with the sensitive region of semiconductor device, and the created charges which around the heavy ion trajectory were collected by sensitive electrode. When

ISSN: 1738-9968 IJHIT

the collected charge exceeds the critical state, the undesirable flip and function confusion will occur, and the device logic state will be flipped, namely original storage "0" into "1", or "1" into "0" [16]. This effect doesn't make the logic circuit damaged. It can also be re-written to another state. Among them, ram, rom and microprocessor, digital signal processor and the programmable logic devices, three components of a set of registers with the internal storage unit is most sensitive to SEE [17].

In this paper, a detected circuit was designed for single particle flip failure of the SRAM. Then, the method of CRC and dual redundant were taken with FPGA to mitigate the SEU. The test results demonstrate that the anti-SEU performance of SRAM was improved. The reference chip is used for comparison with the test chip. The sensitive sites of the SEU can be detected and CRC reinforcing effect proposed in this article can be verified. QuestaSim and logic analyzer simulation test results show that the detected circuit can achieve the aim of the detection of the single particle flip failure of SRAM. The strengthening method proposed in this article can improve the anti-SEU performance of storage chip.

2. SEU Detection Circuit of SRAM

2.1. The Detection System Board of the SRAM'SEU

Altera's Cyclone III EP3C16Q240C8 FPGA is brought as the core of the test system to design the test circuit board. Cyclone III EP3C16Q240C8 FPGA has the advantage of low power consumption, high performance, low price and its internal logic units up to more than 1500, so that it can fully meet the needs of the design.

In the test system, the PC-based data acquisition software communicates with the FPGA by the serial port. In the FPGA, FIFO module, CRC module, data processing module are designed. The FPGA minimum system board and SRAM are designed separately, connected with flexible flat cable, which facilitates that test different types of SRAM chips, so that the design increased the application range of this board .The overall structure of the test system shown in Figure 1:

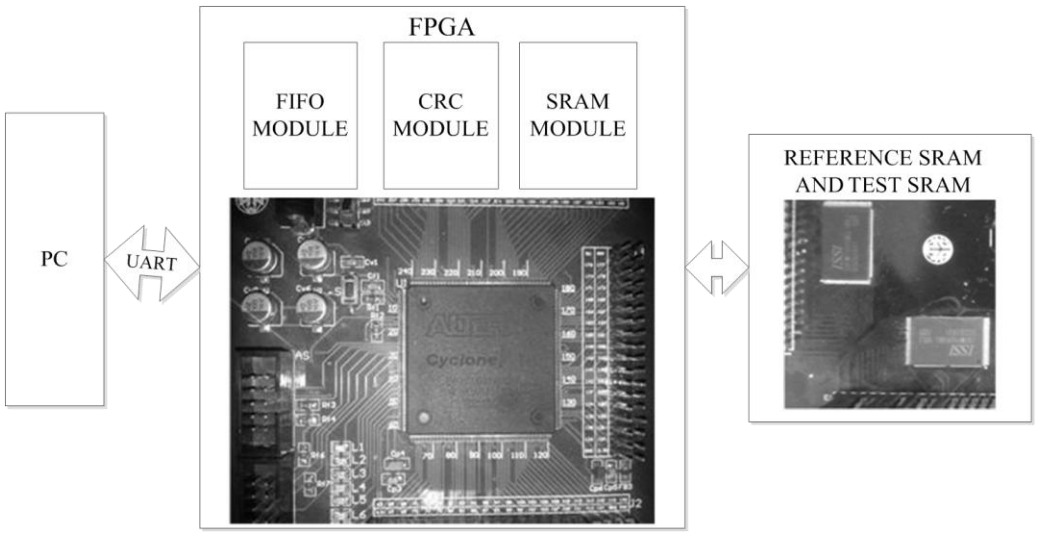

Figure 1. The Overall Structure of the Test System

2.2. The Data Flow of Test System

During the test, the test data is conveyed through the serial port to the FIFO module. After processing by the CRC module, the data starts from the first address of the test SRAM and reference SRAM memory through all the SRAM memory cells bit by bit. After the data is processed by the data processing module, the sensitive bits of SEU and its location can be determined. Then the information can be transported through the serial port to the data acquisition software. Data testing process is as follows:

1. The test board is designed based on the FPGA. It will receive the data then put the data into the FIFO, then sent the data at the same time to the same address of the memory cell of the two SRAM.

2. Check the CRC code in reference SRAM.

3. If the checksum is incorrect, discard this data, repeat step 1.

4. If the checksum is correct, read the two SRAM data, and outputs the comparison result.

5. The result is analyzed and which one or several sites in the storage address that had SEU taken place can be showed.

The essential data flow chart as Figure 2.

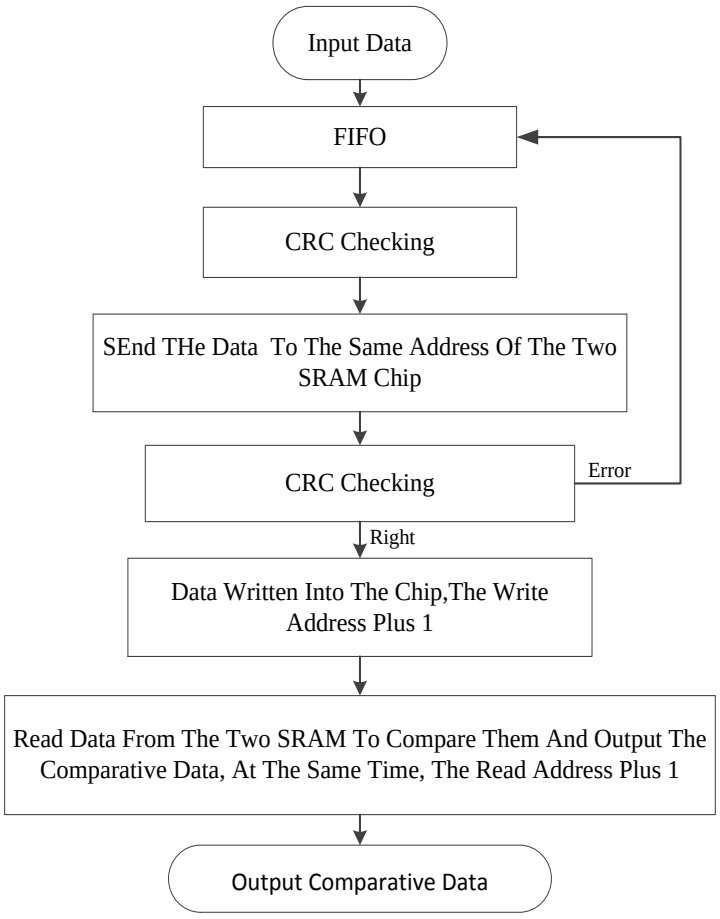

Figure 2. Essential Data Flow Chart

3. The Design of the Logic Module Inside the FPGA

3.1. Serial Transmission and the Section of FIFO

This design uses the serial port for data transfer [18]. Serial port possesses the advantages of simple and easy to debug. FIFO uses Altera's intellectual property (IP) cores. IP core will be used in the circuit, but some of the more complex functional modules designed to modify the parameters of the module. It has good versatility, high accuracy and has good portability. The use of the IP core can avoid duplication of labor and greatly reduce the burden of the engineer. In this article, the FIFO which is used has been proved to be correct.

In this design, through the serial port, host computer transfers data into the FIFO buffer, waiting for the CRC check module to get the signal. When get the signal, a data can be extracted to processing CRC.

3.2. CRC Checking Module

CRC (Cyclic Redundancy Check) is a cyclic redundancy check code. It is an important class of linear block codes. It has the advantages of the simple encoding and decoding method, error detection and error correction ability, so it is widely used in the field of error control in communication [19, 20]. The generation process of the specific checksum shows as follows: Suppose that the n bits data transported are represented by polynomial. The n-k bits left m(x) can be expressed as $m(x) \times 2^{n-k}$. So n-k empty bits are in the right of m(x), and it is the position of the check code. The $m(x) \times 2^{n-k}$ by the generator polynomial g(x) to obtain a quotient Q(X) and a remainder r(x), which remainder r(x) is the check code .namely:

$$\frac{m(x) \times 2^{n-k}}{g(x)} = Q(x) + \frac{r(x)}{g(x)} \quad (1)$$

When the sender sends the data, the information code and the remainder are sent together. A set of information codes and the remainders is called an element; Setting to T(x), then:

$$T(x) = m(x) \times 2^{n-k} + r(x) \quad (2)$$

At the receiving end, any set of polynomial T(x) should be divided exactly by generator polynomial g(x). If errors do not occur in the process of transmission, receiving element and send element are the same. So receiving element must be divided exactly by generator polynomial g(x). If errors occur during transmission, the received element may not be divided. Basing on whether the remainder is zero, we can judge whether errors have occurred in the receiving element.

In this article, CRC checking rules are used in reinforcement design of SRAM chips' SEU, so that the performance of resistance to SEU can be improved. Firstly, data is transported from the FIFO to CRC module. Then the data that is added parity code is sent to a certain storage cell of the test SRAM. The same data without parity code is sent to the same storage cell with the test SRAM in the reference SRAM. Subsequently the data in the SRAM cell is tested to check that whether the received data is correct. If the received data is not correct, the data could be sent again. If the received data is correct, the data without parity code which is extracted from the test SRAM is compared with the data in the same storage cell of the reference SRAM.

The flow diagram of the CRC check reinforcement is shown in Figure3

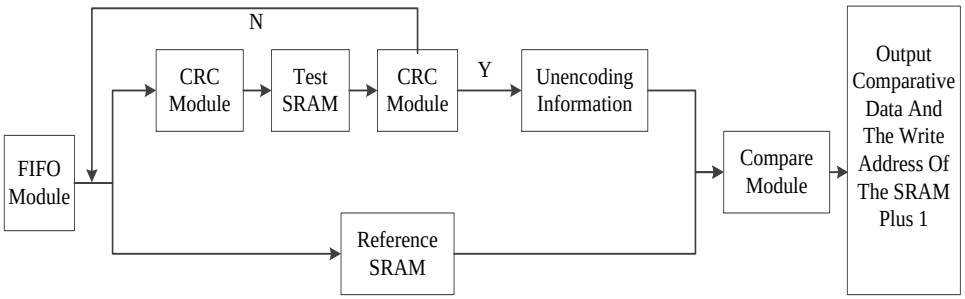

Figure 3. CRC Checking Reinforcement Flow Chart

3.3. Dual Redundant Module

The main function of the compared module is that compare the data in the same storage cell of the two SRAM. So that whether the memory cell is sensitive to SEU can be determined and the comparison result is attached to the output data (the data in the reference data), so that it is facilitate to be detected by the data acquisition software.

The design of the test circuit is that the parity bits are attached with data bits. Parity bits are equal length with data bits. Parity bits are the results of the data of the test SRAM exclusive-or the data of the reference SRAM. The parity bits with the output data are transported in together. If the comparison results are the same, then the parity bits attached by the output data all are 0. If the comparison results are different, then the parity bit corresponded the different bit is 1.

4. Analysis of Simulation Result

4.1. Simulation Test Results of SEU Fault Detection Circuit

First, QuestaSim is used to simulate the detection circuit of SEU. As shown in Figure 4. In the experiment, the data is transported in serial port protocol. Dual redundant modules are designed so that the circuit can determine whether an error occurred. As can be seen from the diagram, if the bit flipping does not occur in the process of data transmission, then the output result data is followed by eight binary 0; If the bit flipping occur in the process of data transmission, then the eight binary data corresponding the bit flipping bit is 1. In Figure 4, the input signal is 11011000, but the received signal appears inverted becomes 11,001,000 (as shown in dashed box), wherein the fifth data bit has bit-flipping. The low becomes a high level. The corresponding bit will be 1 which means that the corresponding data bit-flipping occurred. Thus, the circuit can be designed to detect the occurrence of SEU.

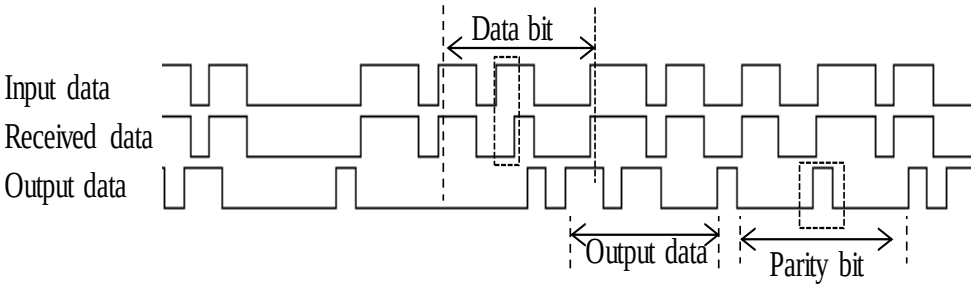

Figure 4. Diagram of the QuestaSim Simulation Test Result

4.2. Logic Analyzer Results of SEU Fault Detection Circuit

In this study, the logic analyzer is used to test the actual output data of the systems. The dual redundant module is used to compare and analyze the results. In Figure5, the bit flipping occurred in the process of the data transition, and the corresponding bit in the parity bits (in the dashed box) is 1. The results are consistent with the simulation results, indicating that the error detection circuit can be designed to achieve the aim of detection of the SEU.

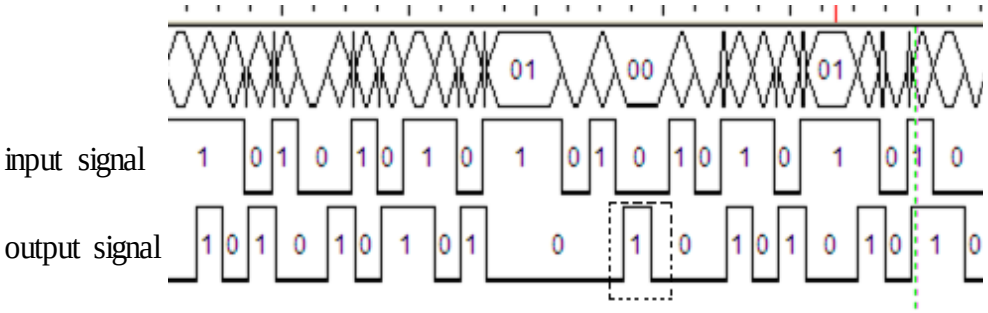

Figure 5. Logic Analyzer Simulation Test Diagram

4.3. The Validation Result of the Method of CRC

The CRC reinforcement design research is carried out in the experiment to reach the aim of reliability and the performance of anti-SEU. The corresponding output data would be affected by the SEU only when the transported data and the CRC code are affected at the same time. Assuming that SEU occurring in each data bit is unrelated. The probability of each of the single event upset is α (α≤1). The probability P_{un_crc} of the occurring of the SEU without the CRC reinforcement design is:

$$P_{un\_crc} = C_8^1 \alpha (1-\alpha)^7 \quad (3),$$

The probability P_{crc} of the occurring of the SEU with the CRC reinforcement design is:

$$P_{crc} = C_8^1 \alpha (1-\alpha)^7 \times \alpha (1-\alpha)^7 \quad (4),$$

$$\frac{P_{crc}}{P_{un\_crc}} \geq \frac{1}{\alpha} \quad (5)$$

The rate of the memory cell bit caused by single event upset is 4.04E-7 (times/bit·days) [21]. Radiation anomalies in the South Atlantic region and the peak of solar activity may increase one or several orders of magnitude in the probability of occurrence. The probability of the occurrence of the SEU selected is 1E-6 and thus the proposed method can improve the performance of the anti-SEU of multiple six orders of magnitude to achieve an effective anti-SEU purpose.

Figure 6 is the simulation of CRC checksum method. As can be seen from the figure 6, the data received by receiving module has no difference with the data received by sending module. When the data received by receiving module is encoded by the CRC module, the flag bit all is 0. So the CRC code can encode the data correctly, and also can check the data correctly, so we can reinforce the design basing on the CRC code.

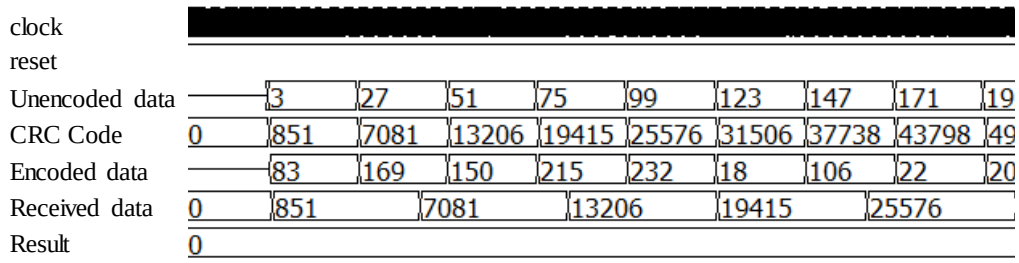

Figure 6. Diagram of the Simulation of CRC Checksum Methods

4.4. The test of the Reinforcement Effect based on the Redundancy Check Method

The test effect of the proposed method's reinforcement is shown in Figure 7. Input data at the cursor is 0001 1110 originally, but bit-flipping occurs during data transfer so the data becomes 010 1110. The sixth bit jumps from 0 to 1. Before the CRC reinforcement, the output data is different from the input data 0001 1110.However, after the CRC reinforcement, the output data is same with the input data .So the reinforcement method can correct the error that cased by the SEU. Thus the error caused by the SEU can be well corrected by the proposed method to reach the purpose of effective resistance to SEU.

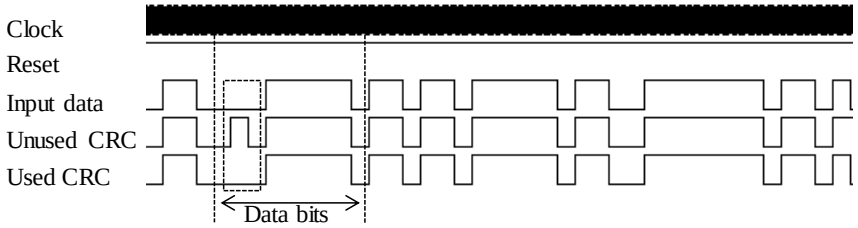

Figure 7. Diagram of the Test Effect of the Proposed Method's Reinforcement

Figure 8 is the real-time sampling picture by the logic analyzer. When data flipping has occurred in input data, the toggle bit without CRC cannot be corrected ,while the toggle bit with CRC can be corrected (as shown in the dotted box below).

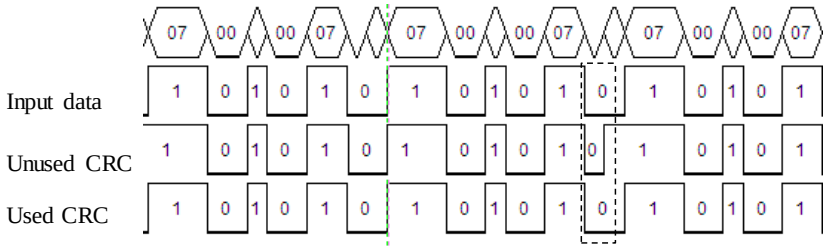

Figure 8. Analysis Diagram of the Logic Analyzer

Thus the dual redundant module is a good way to correct the toggle bit caused by SEU. It improves the ability of anti-SEU of the storage unit. At the same time, it illustrates that this test system has the realizability.

5. Conclusion

In this article, a SEU failure detected circuit is designed for the failure of the SEU and dual redundancy and CRC approach was used for reinforced circuit. The designed circuit could traversal all the address of the memory chip. The address of the memory cell can be detected so that you can detect failure early to safeguard the reliability of airborne equipment and make the potential risks and losses to a minimum stage. As can be seen from the results of detected circuit, the performance of the anti-SEU of the SRAM chip can be improved in some extent based on the proposed reinforcement method with CRC and dual redundancy. The performance of the anti-SEU can be well improved by the proposed method. This experiment is the basic research of the anti-SEU of the memory chip. For more complex anti-SEU research, it has very important significance.

Acknowledgements

This paper was funded by "Joint Fund of the National Natural Science Foundation of China and the Civil Aviation Administration of China (No. U1333120), the Fundamental Research Funds for the Central Universities of China (No. 3122014C025), the Fundamental Research Funds for the Central Universities of China (No. 3122013P004), and the Research Startup Foundation of Civil Aviation University of China (No. 2012QD26X)".

References

[1] F. L. Kastensmidt, L. Sterpone, L. Carro and M. Sonza Reorda. On the optimal design of triple modular redundancy logic for SRAM-based FPGAs. Proceedings -Design, Automation and Test in Europe, **(2005)** March 7-11; Munich, Germany.
[2] Y. Tan, H. Yang and J. Huang. Voter insertion algorithm based on critical path for triple module redundancy. Dianzi YU Xinxi Xuebao/Journal of Electronics and. vol. 34 **(2012)**, pp. 487 - 492.
[3] O. Ruano, J. A. Maestro and P. Reviriego. A fast and efficient technique to apply Selective TMR through optimization. Microelectronics Reliability. vol. 51, no. 12 **(2011)**, pp. 2 240-2388.
[4] C. A. Argyrides, P. Reviriego and D. K. Pradhan. Matrix-based codes for adjacent error correction. IEEE Transactions on Nuclear Science. vol. 57, no. 4 PART 1 **(2010)**, pp. 2106 -2 211.
[5] X. She, N. Li and D. W. Jensen. SEU tolerant memory using error correction code. IEEE Transactions on Nuclear Science. vol. 59, no. 1 PART 2 **(2012)**, pp. 205 - 210.
[6] K. F. Zhang . Research of Resistance to Single Event Upset Effect for Static Access Memories. Modern Electro nics T echnique. vol. 34 no. 18 **(2011)**,pp.60-63.
[7] J. P. Xiong, H. B. Jia and Z. You. Detection and Correction of SEU in the Data-Handling System of Mi cro-Satellite. CHINESE S paces Science And Technology. vol.6**(2000)**,pp.50-56.
[8] C. Gao, W. Guo and J. Huang. Single-Event-Upset (seu) mitigation techniques for routing resources of SRAM-FPGA. International Journal of Advancements in Computing. vol. 4, no. 20 **(2012)**, pp. 205 - 213.
[9] K. C. Coulie, H. Aziza and G. Micolau. Optimization of SEU simulations for SRAM cells reliability under radiation. Journal of Electronic Testing: Theory and Applicat. vol. 28, no. 3 **(2012)**, pp. 331 - 338.
[10] L. Sterpone. SEL-UP: A CAD tool for the sensitivity analysis of radiation-induced Single Event Latch-Up. Microelectronics Reliability. vol. 53, no. Langford Lane, Kidlington, Oxfor **(2013)**, pp. 1 131-1311.
[11] N. A. Dodds, N. C. Hooten and R. A. Reed, Effectiveness of SEL hardening strategies and the latchup domino effect. IEEE Transactions on Nuclear Science. vol. 59, no. 6 **(2012)**, pp. 2 265-2642.
[12] V. Lalucaa, V. Goiffon and P. Magnan, Single-event effects in CMOS image sensors. IEEE Transactions on Nuclear Science. vol. 60, no. 4 **(2013)**, pp. 2 250-2494.
[13] J. Chen, S. Chen and Y. He. Novel layout technique for single-event transient mitigation using dummy transistor. IEEE Transactions on Device and Materials Reliabil. vol. 13, no. 1 **(2013)**, pp. 177 - 184.
[14] D. Li, J. Qin and S. Chen, The dependence of process parameters on single event transient in 25 nm FinFET. Guofang KEJI Daxue Xuebao/Journal of National UNIV. vol. 34, no. 5 **(2012)**, pp. 127 - 131.
[15] D. Mcmorrow, R. Magno and A. S. Bracker, Charge-collection dynamics of AlSb-InAs-GaSb resonant interband tunneling diodes (RITDs). IEEE Transactions on Nuclear Science. vol. 48, no. 6 I **(2001)**, pp. 1 197-1973.

[16] D. Rennie, D. Li and M. Sachdev, Performance, metastability, and soft-error robustness trade-offs for flip-flops in 40 nm CMOS. IEEE Transactions on Circuits and Systems I: Regular Papers. vol. 59, no. 8 **(2012)**, pp. 1626 - 1634.
[17] X. Kefei, Y. Jianwei and Z. Chuangshen, Single event upset induced multi-block error and its mitigation strategy for SRAM-based FPGA. Science China Technological Sciences. vol. 54, no. 10 **(2011)**, pp. 2657 - 2664.
[18] Z. H. Xin, X. Y. Wu and Q. Zhang, Research on the communication of the serial port between the host personal computer and CC2430. Advanced Materials Research. vol. 791 **(2013)**, pp. 1974 - 1977.
[19] H. Fan, S. Wang and Y. Zhu, CRC coder-encoder algorithm and its FPGA implementation. Shuju Caiji YU Chuli/Journal of Data Acquisition a. vol. 21, no. SUPPL. **(2006)**, pp. 97 - 100.
[20]. H. H. Mathukiya and N. M. Patel, A novel approach for parallel CRC Generation for high speed application. Proceedings - International Conference on Communic, **(2012)** May 11-13; Rajkot Rajkot.
[21] Y. Bentoutou and A. S. Mohammed, A review of in-orbit observations of Radiation-Induced effects in commercial memories on-board Alsat-1. Proceedings of World Academy of Science, Engineeri. vol. 66 **(2012)**, pp. 709-711.

Authors

Peng Wang was born in 1982. He obtained his master degree in ENSICA (École Nationale Supérieur d'Ingénieurs deConstructions Aéronautique) in 2005.

Now he is working in Airworthiness Certification Technology Research and Management Center, Civil Aviation University of China, as an associate professor. He mainly engaged in the commercial system security design and evaluation, airborne electronic hardware airworthiness technology research.

Chengxiang Jiang was born in 1988, now is a master's student. He mainly engaged in the mitigation technology of single event upset in avionics application.

Zhen Li born in 1989, now is a master's student. He mainly engaged in civil aircraft research of airborne electronic hardware fault injection method.

Qiannan Xue was born in 1984. She obtained her Ph.D. degree in Institute of Electronics, Chinese Academy of Sciences in 2012. She is a research associate now. She mainly engaged in the study of the radiation effects and hardness of microelectronic devices.