A BRIEF DISCUSSION ON ELICITING AND VALIDATING REQUIREMENTS TO HANDLE SINGLE EVENT UPSETS IN ONBOARD AEROSPACE ELECTRONICS

Sérgio Roberto Ferreira Machado

National Institute for Space Research – INPE/DMC
sergio.roberto@anac.gov.br

Marcelo Lopes de Oliveira e Souza

National Institute for Space Research – INPE/DMC
marcelo@dem.inpe.br

Abstract: Since the dawn of space age, onboard aerospace electronics has suffered many types of interferences when flying in high altitudes. This successively happened with balloon payloads, experimental planes, rockets and satellites. Today, it starts happening with aircrafts, since *avionics systems are increasingly used to perform safety-critical functions at high altitudes. But their increasing capacity and concentration of memory and logics leads to more frequent occurrences of single event upsets, especially in high altitudes. In this work we briefly discuss the process of eliciting and validating requirements to handle single event upsets in avionic systems. To do that, we present the radiation environment of the atmosphere, radiation induced errors, single event upsets, etc., and some of the effects on avionic systems and ways of mitigation, reported in the literature. Finally, we discuss the provisions to demand the adoption of such mitigation measures, and their sufficiency by transforming them into requirements. This will help in the process of eliciting and validating requirements to handle single events upsets in avionic systems.*

Keywords: *Avionics, Radiation Effects, Single Event Upsets, Systems Engineering, Requirements Engineering*

1. Introduction

Today, aircrafts are flying at increasing altitudes due to restrictions of efficiency and cost effectiveness. Flights over the Earth poles are getting more common. Electronic components are getting more integrated and performing more complex functions, demanding extensive use of memories. These factors contribute to the growing of their sensitivity to Single Event Effects-SEEs, demanding mitigating actions.

The definition of requirements based on criticality and reliability criteria, since the initial phases of the development, leads to an optimized project. It means that mitigation techniques for SEEs shall be adequately applied.

This adequacy must be verified by means of application of requirements verification and validation processes to ensure that the models and solutions defined at the early phases are correct and useful.

2. Atmospheric radiation environment

Particles containing very high energy interact with the atmosphere atoms generating the so called secondary particles. Great parts of these particles are neutrons and they are the main responsible for generating the Single Event Effects (SEEs).

These SEEs induced by atmospheric neutrons are known and documented phenomena since 1992, when Normand and Taber (1996) measured the Single Event Upset (SEU) incidence in typical non radiation-hardened Static Random Access Memories (SRAMs) from 30.000 to 65.000 feet and correlated it with the atmospheric neutron environment.

These correlations show that the SEU incidence due to the atmospheric neutron flux varies according to the altitude and latitude, as can be noted in Figures 1 and 2 from the review of SEU collected flight data made by Normand (1996).

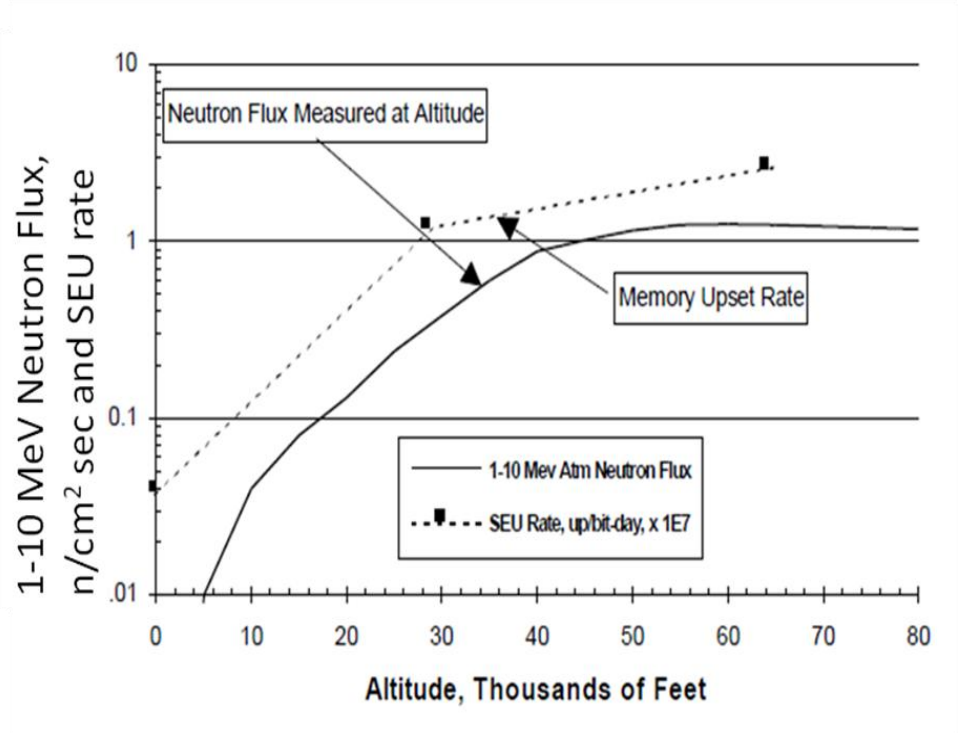

Figure 1: Correlation of the inflight SEU rate in the IMS 1601 SRAM with atmospheric neutron flux as a function of altitude. The SRAM was operated at 2.5V [3].

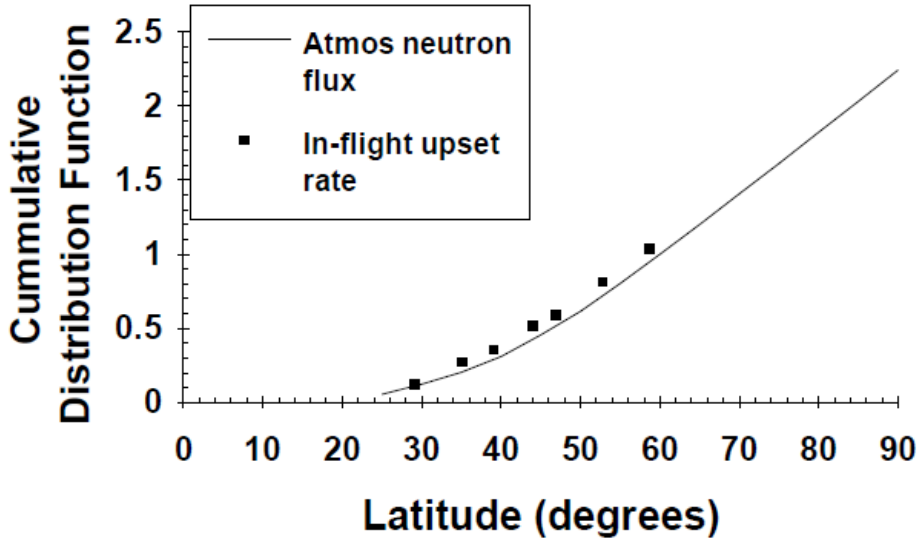

Figure 2: Correlation of the inflight SEU rate in the IMS 1601 SRAM with atmospheric neutron flux as a function of geographical latitude. The SRAM was operated at 5V [3].

3. Effects in onboard aerospace electronics

In general, the process of generation of a SEE involves the interaction of a single particle with a device. For the atmospheric environment considered in this paper, this interaction is not direct, as the neutron does not have a positive or negative charge.

According to NASA (1996), the most common types of SEE are related as follows:

Single Event Latchup (SEL): is a potentially destructive condition involving parasitic currents which can exceed the maximum value supported by the component, leading to the loss of the component, if there is no current limiting. Hence, this effect can be considered either transitory or permanent.

Single Effect Transient (SET): happens when a particle generates a spurious signal that can or cannot become a SEU, in an analog or digital component. It depends of factors as the structure of the component and the clock speed.

Single Event Burnout (SEB): is a destructive condition that can occur in semiconductor power devices which operates in high voltages.

Single Event Functional Interrupt (SEFI): is a kind of SEU in a device, usually complex, where the particle reaches a critical section (for instance, of control, program counters, etc.), in a manner that this section stops to perform adequately.

Multiple Bit Upset (MBU): happens when a particle interacts with the component to change the state of more than one bit. It is more common in memory devices.

Single Event Upset (SEU): is a change in the state of a bit; or it is a transient in a component, inducted by the particle. It is considered a transitory effect, since the rewriting or reset of the device recovers its normal behaviour. This is the most considered and analyzed effect for avionics equipment, because it is the most frequent.

To quantify the SEU rate in an avionic device, we need to know the atmospheric neutron distribution and the cross section of the device, which is the number of upsets divided by the fluency of particles (p/cm^2, particle flux integrated over the exposure time, in general given in units of cm^2/device or cm^2/bit) to which the device was exposed. Then these factors may be multiplied to obtain the SEU per device, as reported in the IEC 62396-1 (2006):

> *SEU rate per device-hour = number of neutrons per area per time (n/cm^2 per hour) × SEU cross section (cm^2 per device).*

The integrated neutron flux varies according to the altitude and latitude, and may be adjusted according to a standardized approach like the described in IEC 62396-1Annex D.

4. Some mitigation techniques

Since shielding is deemed to be impractical to avoid SEUs, mitigation techniques shall be used to maintain aircraft functions. The robustness of these techniques can be relaxed when assessments of function's criticality based on safety are made. Some mitigation techniques are described as follows:

1) The design of radiation-hardened electronic components to endure the ionizing radiation effects. But these are more commonly used in the space environment, due to availability and cost.

2) Measures at structure and circuit level of the component. But they demand the detailing of such components and basic cells of the integrated circuits.

3) The detection of SEUs is an important step to avoid its hazardous effects. But how to treat this data is fundamental. In general, one initial approach would be the recovery without the need of a reset, by means of discarding the data or rewriting a memory, for instance. In the impossibility of that measure, one circuit or system reset can be the second step to solve the problem. In the last instance, one power switching could be done, but this must have to be done automatically, since it is not anticipated that the pilot executes such function.

4) The parity check is one of the simplest methods of data verification, where usually is added one bit in the data structure in a way that the data is consistent with the parity, being even or odd. For instance, if the parity is even and the number of "1"s bits is three, the additional bit would be "1" for consistency. This technique is capable to detect error in one bit only, and it is not possible to correct it.

5) The use of cyclic redundancy involves use of modulo 2 arithmetic, where the position of each bit corresponds to a polynomial power with the coefficients being the data (0 or 1), that are divided by a generating polynomial. In this manner, one change in one bit changes the cyclic redundancy. As the parity check, this technique is only for error detection and not correction.

6) The Hamming code is used in many versions and variations. Basically, the technique consist in inserting bits in the data structure to detect eventual errors and correct then with a certain effectiveness, being considered an Error Detection And Correction (EDAC) code. In accordance with the inserted bits, the quantity of detectable and correctable bit varies, so it can be a code, for instance, which corrects one bit and detects two wrong bits.

7) Watchdog timers can be implemented via software or hardware, or a combination of both. It consists in monitoring the status of device or a functional block, and that block in response must send a message indicating its correct functioning. If, after a determined time, the watchdog don't receive the indication of correct functioning, the device or functional block is considered failed and an action will be taken (reset of the device, switching to a redundant functional block, etc.).

8) Hardware redundancy is commonly used in various critical aircraft systems. It can be duplicated, triple or quadruple redundancy, being a potentially effective means of SEU mitigation. One voting scheme can be used when there are at least three circuits in such a way that the output will be the value voted by at least two of the circuits. The Triple Modular Redundancy (TMR) uses a voter, which elects which of the data to be considered. In the case of one circuit failure, the remaining keep the system working, and the fault is corrected and masked. This scheme demands use of a highly reliable voter, because if the voter fails, all the system will fail.

9) Another type of redundancy, the temporal, can be used to obtain a voting scheme, performing the reading of a data in a temporally spaced fashion. For instance, to read a data from a sensor, three samples spaced in time are collected and sent to a voter, which will decide, in case of a discrepancy considered relevant, what the correct data is.

Of the various aircraft systems that performs critical functions the flight control system has gotten more attention and has required sophisticated architectures to implement the fly-by-wire concept to comply with safety objectives such as availability, independence and reliability.

For instance, the Boeing 777 fly-by-wire system comprises three Primary Flight Computers (PFCs), each of which having three similar lanes with dissimilar hardware and the same software. Voting techniques with different comparisons for each type of data are used to detect discrepancies or disagreements. To actuate the flight control surfaces, the Actuator Control Electronics (ACEs) receive data from multiple ARINC 629 data buses and directly drive the surfaces. Another philosophy is used for the Airbus A 330 and 340, comprised of three Flight Control Primary Computers (FCPCs) and two Flight Control Secondary Computers (FCSCs), each group having different internal architecture and hardware. Every flight control computer has a command and a monitor element with different software (Moir and Seabridge, 2008).

As illustrated above, many mitigation techniques can be combined to achieve the safety objectives. Such combination requires a structured approach to deal with risks like the SEUs.

5. Provisions to demand the adoption of mitigation measures

In Brazil, the transport category airplanes must comply with the requirements of Brazilian Civil Aviation Regulations (RBAC) 25. This regulation adopts the integral text of the Title 14 of the Code of Federal Regulations (CFR) Part 25 of the Federal Aviation Administration (FAA). But in none of the requirements applicable to the various airplane systems there is a requirement explicitly demanding that an avionics system be protected against the prejudicial effects due to SEUs.

The item 25.1309 is a requirement applicable to general systems, installations and devices of the airplane. It demands evidence that they must have an acceptable level of safety, taking into consideration effects and combination of failures. It also must be shown that there must be no simple failure, regardless of the probability of occurrence, of any element, who leads to a catastrophic condition. The final objective is to obtain a fail-safe airplane. To show compliance, there must be an extensive safety assessment. This is a systematic and comprehensive process of evaluation of the airplane to show that its project is in accordance with the fail-safe philosophy, therefore complying with safety requirements.

The Advisory Circular AC 25.1309-1A is a guide which provides an acceptable means, but not the only means, to show compliance with the item 25.1309. The Aerospace Recommended Practice ARP 4761 (1996) assists in detailing the safety assessment process, while the ARP 4754 A (2010) is a guide to certify systems considered complex or highly integrated. The term "complex" refers to systems whose safety cannot be shown solely by test and whose logic is difficult to comprehend without the aid of analytical tools. The term "highly integrated" means that the system executes or contributes to multiple aircraft-level functions. In this context, the analytical methods prescribed in this entirety of standards could receive the derivate values of failures due to SEUs of

electronic systems for consideration in the quantitative analysis of the safety assessment. However, the ionizing radiation environment is not taken into account in such analysis.

The Directive Ordnance DO 160 (2010), accepted by FAA by means of AC 21-16, is the most used standard for test procedures and environmental conditions (such as vibration, fire, electromagnetic interference, etc.) for airborne equipment, containing acceptable environmental qualifications to show compliance with certain airworthiness requirements. The Special Committee 135 of RTCA Inc. is responsible for the standard review, and has discussed the creation of a new chapter considering effects of atmospheric radiation, which can contribute for the adoption of radiation immunity requirements for avionics systems.

The electronic airborne hardware must demonstrate that it executes its function in a safely manner, in a specified environment. One of the accepted means to show compliance is by following the steps prescribed by DO 254 (2000). For airborne software, DO 178 C (2011) is used.

The project requirements generated in the DO 254 process are determined in accordance with the severity classification of the failure condition of the electronic hardware, in the same manner as in ARP 4761 for systems in general: level A – catastrophic, B- hazardous, C – Major D – Minor and E – no effect. The process will be more or less rigorous if the hardware would be complex (every device that is not considered "simple") or simple (the functionalities of the device can be verified by deterministic tests), respectively. Some manufacturers of electronic hardware take into consideration the SEU effects for devices that execute critical functions, but the deepness of this analysis and the generated requirements are unknown. Figure 5 outlines the relations between the main guideline documents covering the development phase:

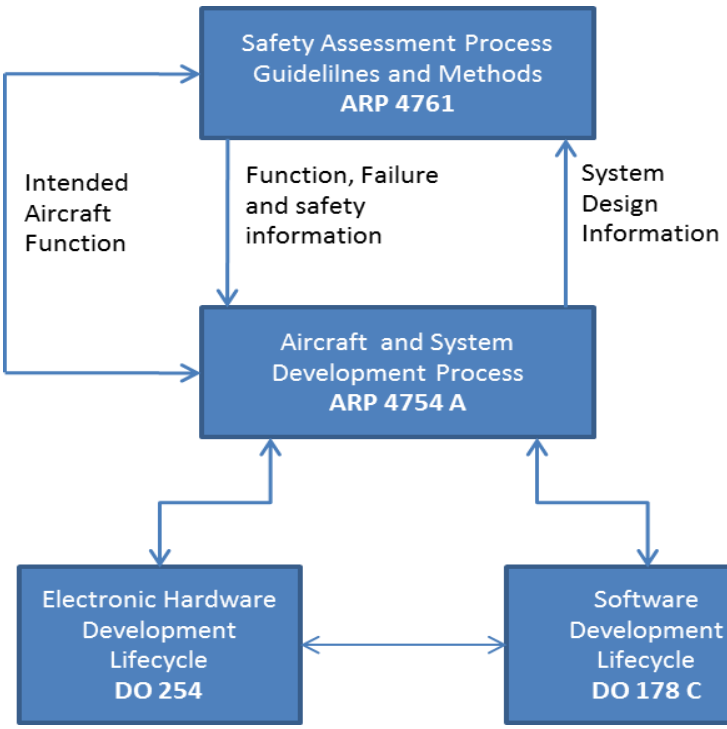

Figure 5: Main Guideline Documents Covering the Development Phase (adapted from ARP 4754 A (2010))

The TS 62396 [12] is a guide to specifically deal with the radiation effects in the atmosphere up to 60 thousand feet of altitude for avionics. It defines the radiation environment, the effects in the electronic devices; and it raises project considerations to tolerate the SEEs. Therefore, its application would lead to demand for adoption of mitigation measures consistent with the ARP 4761 process and would be adequately documented. However, only a few components have data of SEE tests, leading the analysis of systems to adopt conservative approaches, which can produce a demand to take excessive mitigation techniques, so the voluntary adoption of the standard can be difficult.

6. Summary/conclusions

In this work, we discussed some effects and mitigations for SEUs, and some provisions to develop future requirements for avionics systems. The creation of standards, changes in the accepted standards to include

radiation immunity tests and the adoption of project requirements for electronic airborne components by the manufacturers indicate the concern in aviation about SEEs.

Manufacturers of avionics and aircrafts are participating of research groups to understand and develop solutions for the problems caused by the SEUs, generating their own project requirements. They know that the generation of new certification requirements is made by an extensive and analytic process, taking years to its final release.

The elicitation of requirements identifies and quantifies the necessary information to design a safe, complete and coherent system. An approach to deal with SEUs in avionic systems consistent with the process described in guidelines as ARP 4754 A and DO-254 will be proposed in the future as part of a work in progress.

7. References

International Electrotechnical Commission Technical Specification "Accommodation of Atmospheric Radiation Effects Via Single Event Effects within Avionics Electronic Equipment," IEC TS 62396-1 Rev. Mar. 2006.

Moir, I., Seabridge, A., "Aircraft Systems: Mechanical, Electrical and Avionics Subsystem Integration", John Wiley & Sons Ltd, third edition, 2008.

National Aeronautical and Space Administration "Single Event Effect Criticality Analysis (SEECA): The SEECA Document," NASA Goddard Space Flight Center, 1996.

Normand E., "Single-Event Effects in Avionics", IEEE Transactions on Nuclear Science, Vol. 43,No. 461, 1996.

Normand, E., Taber, A. H. "Investigation and Characterization of SEU Effects and Hardening Strategies in Avionics", Defense Nuclear Agency, Alexandria, VA, 1995.

Normand, E., Wert, J. L., Quinn, H., Fairbanks, T. D., Michalak, S., Grider, G., Iwanchuk, P., Morrison, J., Wender, S., Johnson, S., "First Record of Single-Event Upsets on Ground, Cray-1 Computer at Los Alamos in 1976", IEEE Transactions on Nuclear Science, Vol. 57, No. 6, December 2010.

RTCA Inc. "Software Considerations in Airborne Systems and Equipment Certification," RTCA DO-178, Rev. C, Dec. 2011.

RTCA Inc. "Design Assurance Guidance for Airborne Electronic Hardware" RTCA DO-254, Rev. Jan. 2000.

RTCA Inc. "Environmental Conditions and Test Procedures for Airborne Equipment," DO-160G, Rev. Jan. 2010.

SAE International. Aerospace Recommended Practice "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment" SAE ARP 4761, Rev. Dec. 1996.

SAE International. Aerospace Recommended Practice "Guidelines for Development of Civil Aircraft and Systems", SAE ARP 4754 Rev. A, December. 2010.

Telelogic DOORS® Manual "Get It Right the First Time: Writing Better Requirements", IBM® Corporation, 2008.