Field Programmable Gate Array Failure Rate Estimation Guidelines for Launch Vehicle Fault Tree Models

Mohammad Al Hassan, National Aeronautics and Space Administration (NASA); mohammad.i.alhassan@nasa.gov

Paul Britton; National Aeronautics and Space Administration (NASA);

Glen Spencer Hatfield; Bastion Technologies Incorporated, 17625 El Camino Real #330, TX 77058, USA

Steven D. Novack; Bastion Technologies Incorporated, 17625 El Camino Real #330, TX 77058, USA steven.d.novack@nasa.gov

ABSTRACT

Today's launch vehicles complex electronic and avionics systems heavily utilize Field Programmable Gate Array (FPGA) integrated circuits (IC) for their superb speed and reconfiguration capabilities. Consequently, FPGAs are prevalent ICs in communication protocols such as MIL-STD-1553B and in control signal commands such as in solenoid valve actuations.

This paper will identify reliability concerns and high level guidelines to estimate FPGA total failure rates in a launch vehicle application. The paper will discuss hardware, hardware description language, and radiation induced failures. The hardware contribution of the approach accounts for physical failures of the IC. The hardware description language portion will discuss the high level FPGA programming languages and software/code reliability growth. The radiation portion will discuss FPGA susceptibility to space environment radiation.

INTRODUCTION

The digital integrated circuit that makes up the FPGA is based on Complementary Metal-Oxide-Semiconductor (CMOS) technology. This integrated circuit is designed to be configured by the end user or customer after manufacturing. Unlike Application Specific Integrated Circuit (ASIC), FPGAs are designed with the capability to be configured and reconfigured, hence the name "Field programmable". As shown in Figure 1, the internals of the FPGA IC consists of programmable logic blocks and a hierarchy of reconfigurable interconnects that can be inter-wired in different configurations. Those interconnects are made possible through the CMOS-based IC transistors. The user gets to program the hardware of the FPGA by programing the logic structure of the device: logic blocks and interconnects.

In complex electronics, such as those used in the spacecraft, FPGAs are generally used to perform command, control and communication signal functions. The FPGA is used as the interfacing device between the controlling/commanding device (e.g., flight computer) and the commanded component, such as solenoid valves controlling flow from fuel tanks or thrust vector controllers.

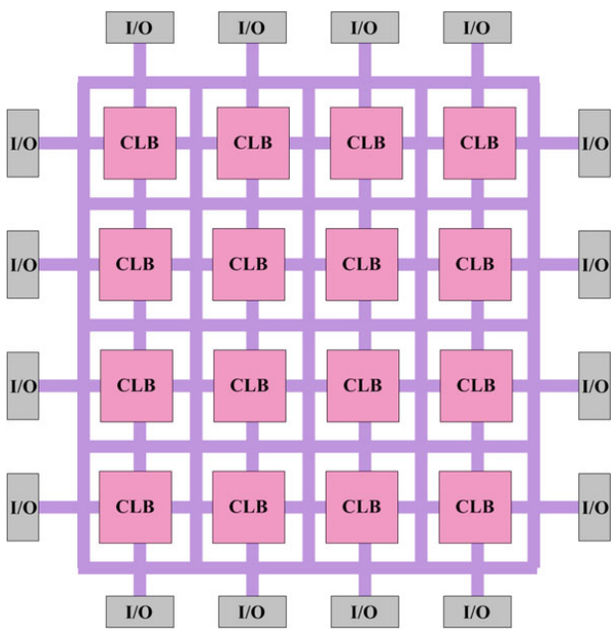

Figure 1. SRAM-Based FPGA Logic Blocks and Interconnects [1]

Herein lies the ability of FPGAs to introduce catastrophic failures for launch vehicles, such as loss of mission, vehicle, or loss of crew. FPGA hardware has the potential to experience different failure modes, such as fail-in-place or fail high/low. Likewise, Hardware Description Language (HDL) coding errors and radiation induced failures have the potential to drive the FPGA to initiate erroneous actuation of the FPGA-controlled components.

1. GUIDELINES TO ESTIMATE FPGA FAILURE RATE

The approach described below aims to provide guidelines to consistently estimate FPGA failure rates across generic spacecraft subsystems. The discussion of this approach will be divided into three sections, hardware, hardware description language code, and radiation effects.

It is important to note that Bayesian updates apply to all three risk contributors discussed in this paper to incorporate data that becomes available from testing and flight operations.

1.1 Hardware Contributions

The bathtub curve, shown in Figure 2, characterizes the hazard function and comprises three parts, infant mortality, useful life, and wear out. The "Infant mortality" steep slope of the curve represents initially high failure rates that decrease with time as defective parts are identified and discarded. The curve then flattens as the failure rate becomes more constant and the curve is referred to as constant failure rate region or useful life region. Eventually, the failure rate increases in the wear out region as age and wear induce failures,

In the Useful Life region, the time between random failures, is a reliability figure of merit known as Mean Time Between Failures (MTBF), MTBF is the inverse of the component's failure rate ($\lambda = \frac{1}{MTBF}$).

Hardware failure rate data sources for an FPGA include historical data, similar component/model demonstrated reliability data, testing, prediction as in MIL-HDBK-217FN2, or expert elicitation.

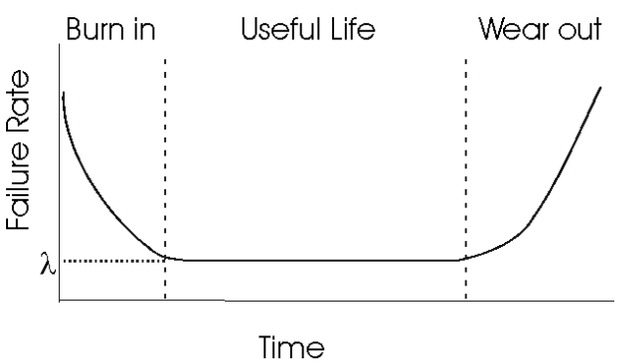

Figure 2. Bathtub Curve Hazard Function for Hardware Failure Characterization

1.2 Hardware Description Language Contributions

The goal of this Section is to provide guidelines to account for failures arising from programming languages used to program FPGAs.

The logic blocks and interconnects of an FPGA are considered hardware, and are programmed/synthesized by programming software such as Very High Speed Integrated Circuit Hardware Description Language (VHDL) or Verilog where the code is subject to software "failure" causes such as bad requirements, programming errors (coding bugs), latent errors, etc. According to NASA Primary Avionics Software System (PASS) report by Johnson Space Center, latent error is defined as "A segment of code that fulfills its requirements except under certain off-nominal, and probably unanticipated conditions" [2]. Latent errors make it past testing and onto operational flights before they are discovered.

It is necessary in this Section to make a distinction between hardware and the software used to program the hardware in terms of failure rate/reliability. This is due to the fact that software and hardware are dissimilar in many aspects. The PASS report [2] points out that software does not wear out over time as hardware does. Software is not susceptible to fatigue or to environmental stressors such as temperature, pressure, shock, vibration and radiation. Therefore, the software hazard function cannot be characterized by the bathtub curve, but is rather modeled with the software reliability curve, as shown in Figure 3.

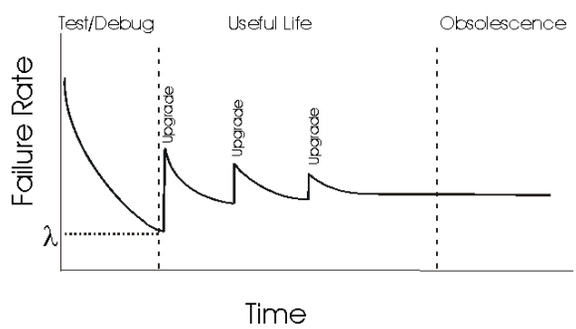

Figure 3. Software Reliability Curve

The Test/Debug region of the curve represents discovery and correction of code faults prior to or during operational use. In the Useful Life region, upgrades introduce new code faults and are evident by the spikes in failure rates. However, the maturity of the code (early mature, mid-mature, and late mature [2]) during Useful Life must be factored in estimating the code's probability of failure. Late-matured code is expected to be the most robust of the three maturity levels. Software risk assessment is often considered relatively more difficult than hardware risk assessments, and every spaceflight program with an interest in quantifying

FPGA HDL risks would need to leverage historical data, test data, and prediction data when possible. Finally, in the Obsolescence region, no more upgrades to the code are conducted and the failure rate in this region becomes entirely driven by latent errors.

1.3 Space Radiation and FPGAs

Space environment is characterized by different sources of radiation that exist within the various space environments (e.g., South Atlantic Anomaly, or Van Allen Belt). Ionizing radiation, has the potential to strip off electrons from the molecules they interact with, hence the name "ionizing radiation". Listed below are the most common types of radiation found in space [3].

I. Galactic Cosmic Radiation (Cosmic Rays)

This type of high energy ionizing radiation comes from exploding stars (Supernovae), and has strong potential to strip-off electrons or leave ionic tracks in the insulation layer of the gates, and is considered the most damaging. It is very difficult to shield spacecraft components from this type of radiation.

II. Trapped Radiation

Trapped radiation is comprised of highly energetic charged particles trapped in the Earth's magnetic field, also known as the Van Allen Belt. The threat associated with this type of radiation is eliminated once the space vehicle is travelling outside of the Van Allen Belt.

III. Solar Energetic Particles

The source of these particles is the sun and they appear in high intensity. Protection from these high-energy particles is easier than cosmic rays and trapped radiation.

1.3.1 FPGA Hardware and Space Radiation

As mentioned above, ionizing radiation deposits energy onto the molecules or atoms it interacts with, and is capable of stripping off their electrons. These high energy particles can interact with the CMOS semiconductor doping of the FPGA, causing erroneous FPGA operation, which poses a threat to the spacecraft reliability.

In general, ionizing radiation effects on integrated circuits such as the FPGA, are classified into two categories: Total Ionizing Dose (TID) and Single Event Effects (SEE). TID is defined as the radiation accumulation thresholds before a transistor starts to experience variation in voltage thresholds and its junctions start to leak currents, leading to functional failure of the transistor. The significant sources of radiation in this case varies from trapped electrons, trapped protons, and solar protons. Fortunately, TIDs do not pose a threat to modern spacecraft as their FPGAs may come equipped with radiation hardened technologies that can withstand long years of radiation accumulation.

On the other hand, SEEs are a serious concern to spacecraft and must be accounted for in the fault tree analysis. They are capable of interrupting a data path and/or causing loss of key spacecraft control function (e.g., loss of communication with flight computers, loss of propulsion control or erroneous valve actuation) leading to loss of mission/crew. A SEE occurs when an energetic particle, such as a cosmic ray's heavy ion or a heavy proton in the Van Allen belt strikes the FPGA integrated circuit leading to disruptive effects. SEE comprises two main categories: soft SEEs and hard SEEs. A soft SEE is referred to as Single Event Upset (SEU), and includes data upsets like bit flips to memory cells or transient pulses in the logic circuitry. Hard SEEs are Single Event Functional Interrupts (SEFI) and Single Event Latch-up. (SEL). SEL is considered the most severe case of SEE that leads to physical destruction of the IC. Fortunately, modern designs and technologies of the spacecraft FPGAs have rendered SELs unlikely to occur.

1.3.2 FPGA Programming Technology and Space Radiation

Space-flight FPGAs come in different memory/programming technologies such as flash-based, Static Random Access Memory (SRAM) based or antifuse-based. Flash-based FPGAs and SRAM cells are more vulnerable to TID and SEU, respectively. A penetrating cosmic ray heavy ion has the capability, depending on the material density and shielding thickness, to penetrate and change logic gates voltage thresholds which can lead to changes in the logic structure. However, antifuse based FPGAs are not reprogrammable and are significantly less sensitive to data upsets or damaged by heavy ions at the energy levels found in space [4].

Some modern spacecraft technologies are inclined toward lowering costs by reducing requirements for components physical parameters such as weight, size, and power consumption, without compromising performance. In order to accomplish this objective, ICs like SRAM utilize new technologies including high speed and lower power CMOS and fiber optics, which are very vulnerable to SEEs [5].

1.4 Failure Rates and the Fault Tree

Table 1 below provides the most common data sources to each failure category of the FPGA along with examples to illustrate the expected format of the failure rate or probability of failure (Pf). A typical spacecraft FPGA high level fault tree should conform to the fault tree shown in Figure 4, which illustrates FPGA high level fault tree logic.

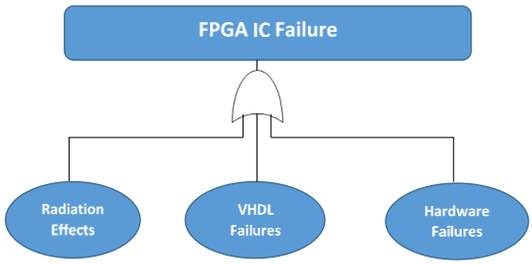

Figure 4. FPGA Fault Tree High Level Logic (OR)

Table 1. Data Sources and Example Failure Rates

Failure Category	Data Sources	Notes	Arbitrary Example Failure Rate/Pf
Hardware	Historical data, prediction methods, and demonstrated reliability data from reliability databases such as EPRD	Modern technology and robust manufacturing techniques have renderred the hardware risk category to be of low-impact, relative to the other two failure categories	1.45 FPMH (68,965 MTBF) *FPMH = Failure per Million Hour
VHDL	Historical data, demonstared data and software prediction programs data	Software reliability growth should be factored in (early mature, mid-mature, and late mature). Failure rate/failure probability is expected to progressively improve with each growth category. The fault tree should account for the most current growth category only	Pf per KSLOC: Early-Mature 7E-06 Mid-Mature 4E-06 Late-Mature 1E-06 *Pf = Probability of Failure * kSLOC = 1,000 SLOC
Radiation	Historical data, demonstared data and SEE prediction programs such as CREME96	The predominant contributor to the SEE prediction is the soft and transient errors (SEU)	500 FPMH (2,000 MTBF)

2. Conclusion

FPGAs speed, configuration flexibility, and cost effectiveness have made the ICs highly sought after in space mission programs to implement high-speed signal processing in spacecraft. However, the FPGAs reliability have been rendered vulnerable to three failure categories: physical hardware, programming-induced failures, and radiation-induced failures. FPGA hardware is an integrated circuit of components with proven reliability track record such as transistors and multiplexors, therefore, it is safe to assume that FPGAs hardware reliability estimates are more reliable than the hardware programming languages and radiation effects by a significant margin. Programming of the hardware logic blocks and interconnects are susceptible to failures introduced to the code including wrong requirements, coding errors, and latent errors. Radiation effects pose a substantial threat to the reliability of the FPGAs and are the predominant risk contributor to FPGA failures [5] in space environment. The ionizing radiation of the space environment interact with the CMOS technology of the semiconductors of the FPGAs. Depending on the energy level of these radiations, the effects could slowly accumulate over the years until a functional failure occurs (TID), or the functional failure could be instant (SEE). In general, an FPGA fault tree should conform to Figure 4 and account for the three failure categories as independent failures (OR logic).

3. References

[1] Farooq, Marrakchi, Mehrez, Tree-Based Heterogeneous FPGA Architecture, Application Specific Exploration and Optimization, 2012, Springer

[2] Russell Robin, Thompson Nelson, Zhu Shangyi, NASA Primary Avionics Software System (PASS) Probabilistic Risk Assessment, SSMA-08-011 Rev. B, August 27, 2010.

[3] NP-2014-03-001-JSC, Types of Radiation in Space, NASA

[4] Kevin Morris, FPGA Reliability in Space-Flight and Automotive Applications, Electronic Engineering Journal, September 6, 2005.

[5] NASA, Goddard Space Flight Center, Radiations Effects & Analysis: https://radhome.gsfc.nasa.gov/radhome/see.htm