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

9th IAASS Conference
Know Safety
No Pain
Toulouse - France
October 18-20, 2017

Mohammad AL Hassan [1]
Paul Britton [1]
Steven Novack [2]
Glen S Hatfield [2]

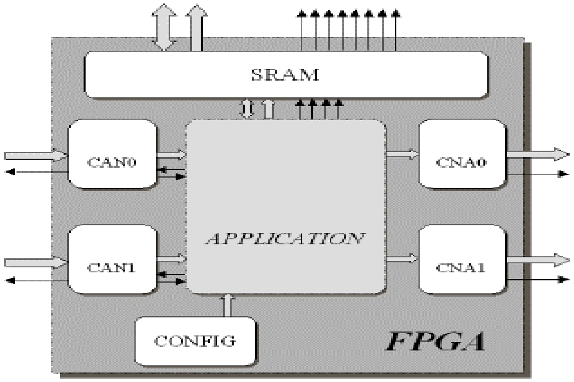
1. NASA, Marshal Space Flight Center (MSFC)
2. Bastion Technologies, Inc.

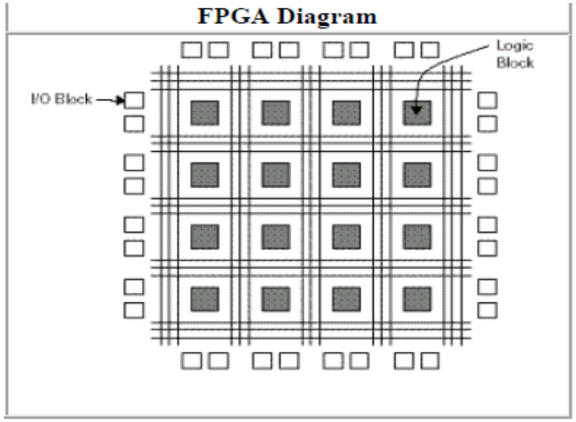
Presentation Outline

- Introduce FPGA and the importance of this Integrated Circuit (IC) in Spaceflight Missions
- Highlight the difference between FPGA and similar technologies (i.e., ASIC)
- Discuss FPGA Failure Ramifications
- Identify Sources of FPGA Failures
- Propose an approach to estimate FPGA Failure Rate

Introduction to FPGA

- Today's launch vehicles complex electronic and avionics systems heavily utilize the FPGA integrated circuits (IC) for their superb speed and reconfiguration capabilities
- The digital integrated circuit that makes up the FPGA is based on Complementary Metal-Oxide-Semiconductor (CMOS) technology
- The IC silicon chip is designed to be configured by the end user or customer after manufacturing
  - hence the name "Field programmable"
  - No soldering or rewiring required to manipulate logic functional blocks
  - This an advantage over Application-Specific Integrated Circuit (ASIC)
- 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.





FPGA Failure Ramifications

- In complex electronics, such as those used in spacecraft and aircrafts, FPGAs are generally used to perform command control and communication signal functions
- Herein lies the ability of FPGAs to introduce catastrophic failures for launch vehicles
- 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

Guidelines for Failure Rate Estimation

- The approach aims to provide guidelines to consistently estimate FPGA failure rates across generic spacecraft subsystems

- This approach will be divided into three sections:
  I. Hardware
  II. Hardware Description Language
  III. Radiation effects

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

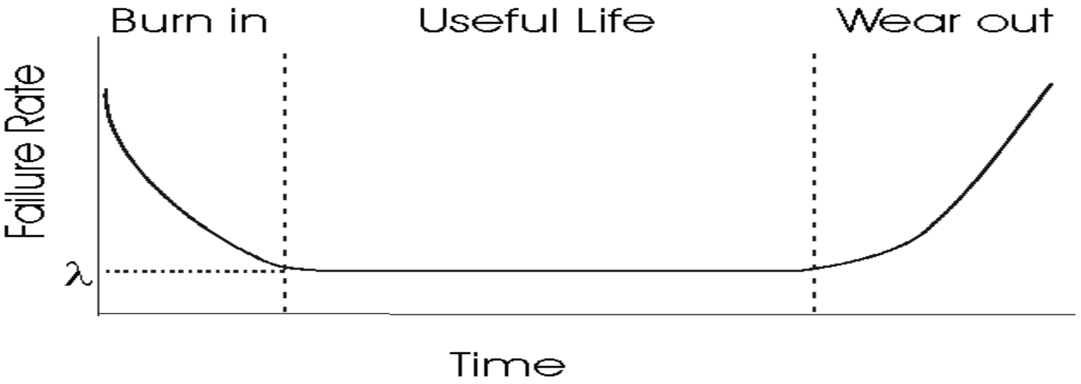
Guidelines for Failure Rate Estimation

I. Hardware Contributions

- The bathtub curve characterizes the hazard function and comprises three parts, infant mortality, useful life, and wear out

- 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.

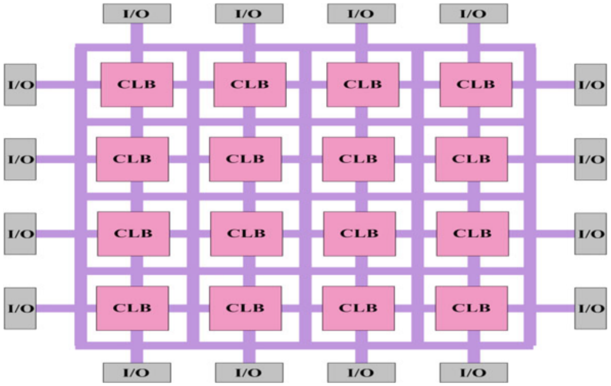


II. Hardware Description Language Contributions

- 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

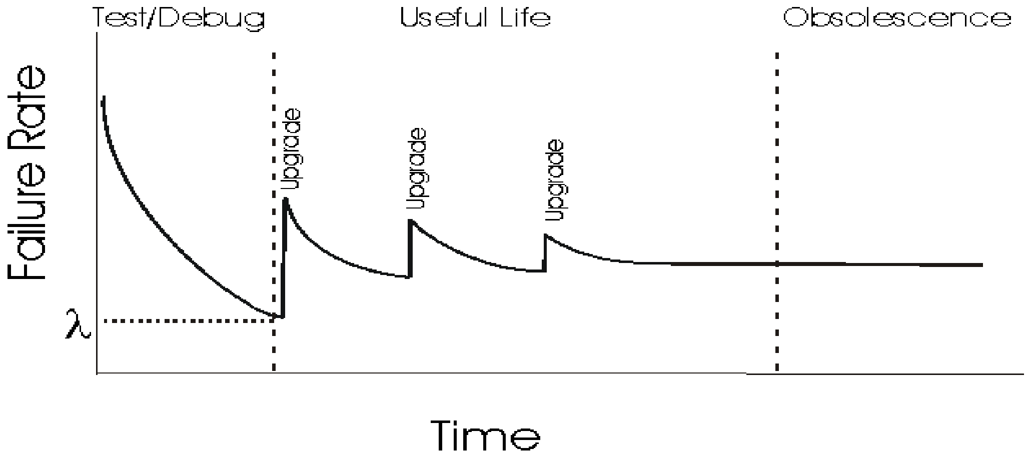
- The code is subject to software “failure” causes such as bad requirements, programming errors (coding bugs), latent errors, etc.



Guidelines for Failure Rate Estimation

II. Hardware Description Language Contributions (Cont.)

- It is necessary 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.
- [2] 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



Guidelines for Failure Rate Estimation
II. Hardware Description Language Contributions (Cont.)

- 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
- Spaceflight programs 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

Guidelines for Failure Rate Estimation

III. Space Radiation Contributions

- 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”
- The next few slides will illustrate the most common types of radiation found in space

Guidelines for Failure Rate Estimation
III. Space Radiation Contributions (Cont.)

- **Galactic Cosmic Radiation (Cosmic Rays)**
  - This type of high energy ionizing radiation comes from exploding stars (Supernovae)
  - Has strong potential to strip-off electrons or leave ionic tracks in the insulation layer of the gates
  - Considered the most damaging. It is very difficult to shield spacecraft components from this type of radiation

- **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

- **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

Guidelines for Failure Rate Estimation
III. Space Radiation Contributions (Cont.)

- Ionizing radiation deposits energy onto the molecules or atoms it interacts with
- These high energy particles can interact with the CMOS semiconductor doping of the FPGA, causing erroneous FPGA operation
- In general, ionizing radiation effects on ICs are classified into two categories:
  - Total Ionizing Dose (TID)
  - 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
- 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

Guidelines for Failure Rate Estimation
III. Space Radiation Contributions (Cont.)

- 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 SEE
  - Hard SEE

- 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)

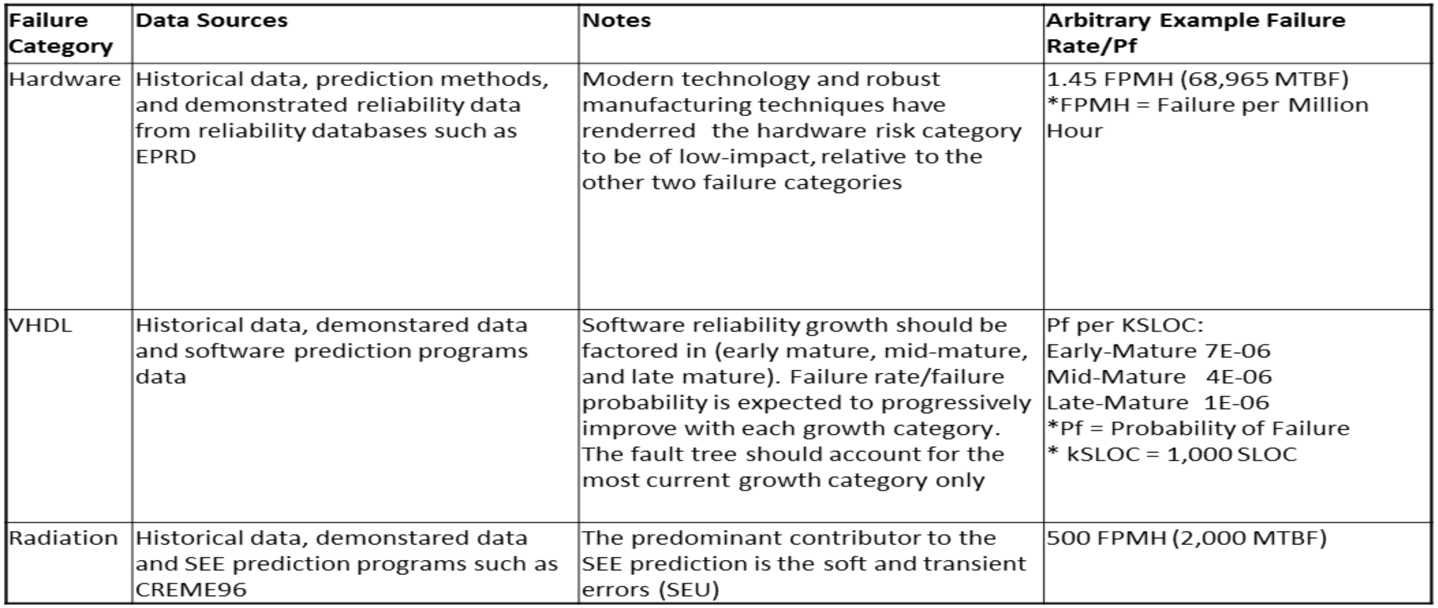
- SEL is considered the most severe case of SEE that leads to physical destruction of the IC. Fortunately, modern designs and technologies of the spacecraft FPGAs have rendered SELs unlikely to occur.

Guidelines for Failure Rate Estimation

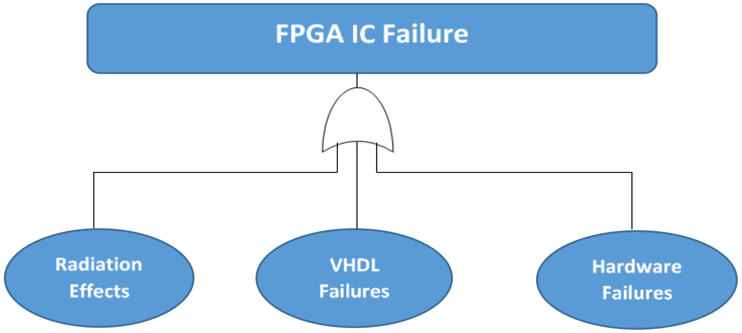
3. Space Radiation Contributions (Cont.)

- 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 to penetrate and change logic gates voltage thresholds
  - 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]

Failure Rates and the Fault Tree



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)



- A typical spacecraft FPGA high level fault tree should conform to the fault tree shown below

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
- Programming of the hardware logic blocks and interconnects are susceptible to failures introduced to the code including wrong requirements, coding errors, and latent errors
- Spaceflight programs with an interest in quantifying FPGA HDL risks would need to leverage historical data, test data, and prediction data when possible
- 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 the high level fault tree shown in the previous slide

Questions?

POC: Mohammad AL Hassan (Mo)

Mohammad.i.alhassan@nasa.gov

Office: +1-256-544-2410