

Unclassified

**Field Programmable Gate Array (FPGA)
Radiation Data:
All Data are Not Equal**

Kenneth A. LaBel

ken.label@nasa.gov

**Co-Manager, NASA Electronic Parts and Packaging
(NEPP) Program**

Melanie D. Berg

melanie.d.berg@nasa.gov

ASRC Space & Defense Inc



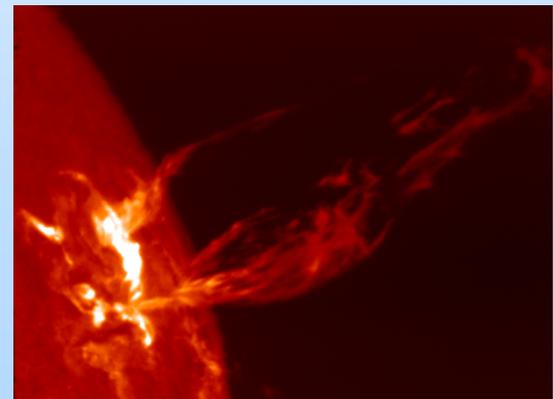
Acronyms

Acronym	Definition
BNL	Brookhaven National Laboratories
CLK	Clock
COTS	Commercial Off The Shelf
DUT	Device Under Test
FPGA	Field Programmable Gate Array
GSFC	Goddard Space Flight Center
IC	Integrated Circuit
IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
JEDC	Joint Electron Devices Council
JEDEC	Joint Electron Device Engineering Council
JTAG	Joint Test Action Group (FPGAs use JTAG to provide access to their programming debug/emulation functions)
NASA	National Aeronautics and Space Administration
NEPP	NASA Electronic Parts and Packaging (NEPP) Program
POR	Power-On-Reset
REDW	Radiation Effects Data Workshop
SEB	Single Event Burnout
SEE	Single Event Effect
SEFI	Single Event Functional Interrupt
SEL	Single Event Latch-up
SET	Single Event Transient
SEU	Single Event Upsets
SEUTF	Single Event Upset Test Facility
TAP	Test Access Port
TCK	JTAG clock signal
TDI	Test Data Input
TDO	Test Data Output
WSR	Windowed Shift Register



Outline

- **Abstract**
- **Introduction**
- **Diatribes 1: Why you may not really understand what a single event functional interrupt (SEFI) is**
- **Tenet 1: The Data**
- **Tenet 2: The Test**
- **Tenet 3: The Analysis**
- **Diatribes 2: Limiting cross-sections**
- **Caveat Emptor!**
- **Discussion**
- **Summary**
- **Acknowledgements**





Abstract

- **Electronic parts (integrated circuits) have grown in complexity such that determining all failure modes and risks based on single particle event radiation testing is impossible.**
- **In this presentation, the authors will present why this is so and provide some realism on what this means to FPGAs.**

It's all about understanding actual risks and not making assumptions.



Introduction

- **Device complexity has increased the challenges related to radiation single event effects (SEE) testing.**
 - **Obtaining appropriate test coverage and understanding of the response of billion-transistor commercial devices, for example, are a concern for every tester.**
 - **This is akin to test vector coverage – have we stimulated sufficient nodes (or states) during our SEE test to understand risk properly?**
- **We present three tenets for FPGA SEE testing to consider:**
 - **Tenet 1: All SEE test data are “good” data;**
 - **Tenet 2: Not all test sets/methods are appropriate or complete; and,**
 - **Tenet 3: Not all interpretation and analysis of SEE data are accurate.**
- **Each of these tenets will be discussed in turn with two related technical diatribes included.**



Diatribes 1:

Single Event Functional Interrupts (SEFIs) – Definitions

- **JEDEC JESD89A* Definition**
 - “A soft error that causes the component to reset, lock-up, or otherwise malfunction in a detectable way, but does not require power cycling of the device (off and back on) to restore operability, unlike single-event latch-up (SEL), or result in permanent damage as in single event burnout (SEB).”
 - An example is an SEU in a control register changing operational modes of a device.
- **Modern integrated circuits (ICs) are not that straightforward (see next chart)**

***Joint Electron Devices Council (JEDEC) -
Measurement and Reporting of Alpha Particle and
Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices
(note: soft errors are terrestrial version of single event upsets (SEUs))
(also note that JESD57 is developing an updated definition)**



Diatribes 1 – SEFIs?

- **Are these SEFIs?**
 - **An SEU in hidden circuitry**
 - May not change apparent device operation, but is observed via changes in power consumption (power cycle may be required to recover),
 - **A single event transient (SET) in a power-on-reset (POR) circuit that power cycles/resets the device**
 - Problem clears itself, but there is down time and to-be-determined operating state after recovery,
 - **An SEU that latches in a redundant (weak or flawed) row/column in a memory array**
 - May not be recoverable by power reset, or
 - **An SEU in a security block**
 - Device may continue working, but user's ability to change modes may be disabled.
- **We'd say YES and all of these are potential *FPGA* concerns!**



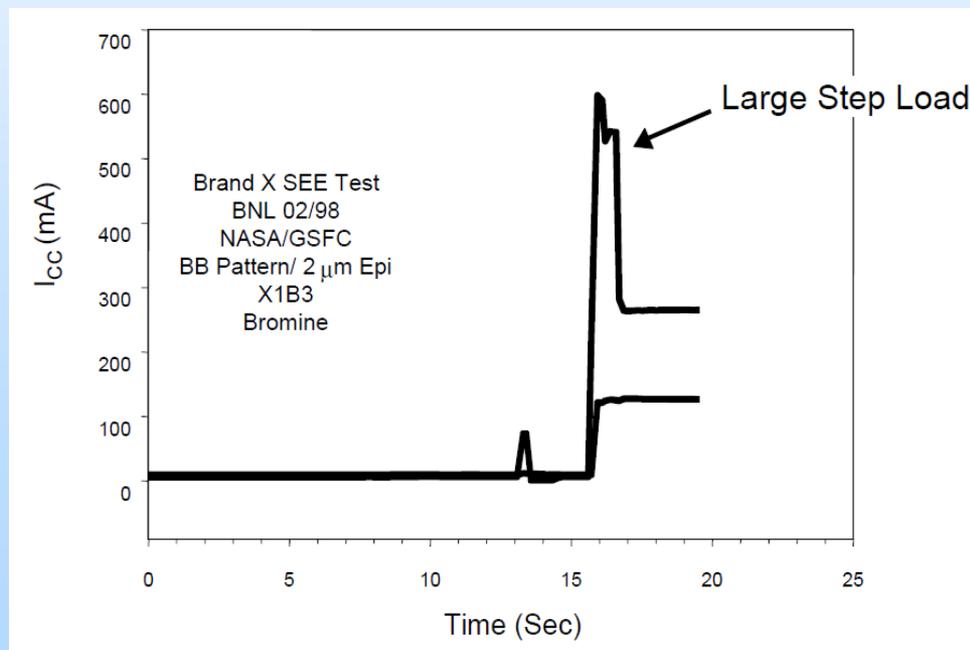
Diatribes 1: SEFI – The Term

- **Originally coined in the mid-1990s by Gary Swift (then at Jet Propulsion Laboratories) to describe a class of SEUs (or a propagated SET) that causes a functional “hiccup” to occur and may be “soft” (can be cleared by reprogramming, restarting, or other non-power cycling means) or “hard” (requires power cycle).**
 - **Operational changes would be included as well as those “non-operational” changes like current creep.**
 - **This is a more general description than the JEDEC definition.**



A SEFI Example (1)

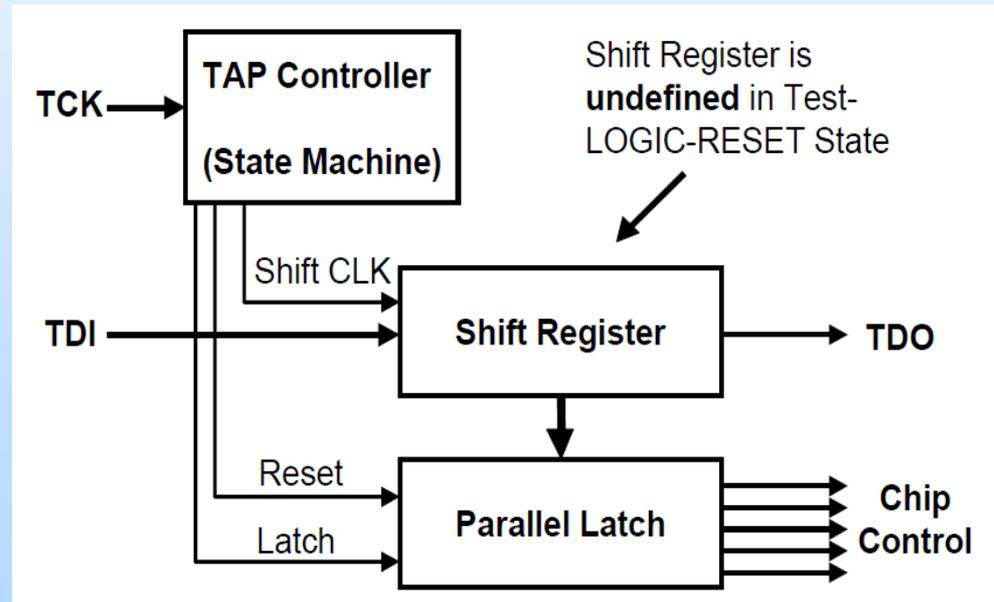
- The figure below illustrates a step load increase in the power consumption (supply current) that occurred during an SEU test on an ancient FPGA device (Katz, et al).
 - Single event latchup (SEL) is often assumed when power increased as observed.
 - Device configuration also was altered during the event.





A SEFI Example (2)

- The SEFI event was associated with the built-in circuit for the International Electrical and Electronics Engineers (IEEE) Joint Test Action Group (JTAG) 1149.1 Test Access Port (TAP) controller as illustrated below.





A SEFI Example (3)

- The bottom line is that the observational line between a SEFI and SEL can be very blurry.
- Without a true understanding of the device's operation (for both areas accessible to the user and those that aren't) as well as a maximization of *visibility by the test set/method*, understanding and classifying an event may be problematic.



Tenet 1: The Data are Always “Good”

- In short, data are just data.
 - It is what was observed and captured during an SEE test.
 - Now the question becomes: are the data captured complete, appropriate, and interpreted correctly?
- Think of the questions this brings into play:
 - Have all data points been captured? (**adequate and reliable data capture**),
 - Was the test prognostic enough to gather the right range of data (think of the simple SET capture from an operational amplifier – was the minimum pulse width/amplitude sensitivity of your oscilloscope set appropriately)? (**appropriate test set granularity**); or,
 - Have all the right test vehicles/designs been used to generate that data? (**adequate test circuits/operation**)

The point is simple: the data are correct, but there's either not enough of it or insufficient granularity of information.

The simple takeaway is that testing requires a look far below the surface...



Tenet 2: The Test (1)

- The first complication comes from the way the device under test (DUT) is tested and the way data capture was performed.
- The general idea is to focus on **prognostic** testing – ensuring that your test design is inquisitive enough to capture all available information on an event and about relevant areas within the DUT.
 - This runs counter to “testing your flight design” and is needed due to the nature of *accelerated* ground test environments.
- We will define design *visibility* as ensuring that the interface between what the DUT is doing and how the test system is operating is adequate to capture all relevant event information.



Tenet 2: The Test (2)

- **While this presentation isn't a "how-to-test" document, it does recommend a thought process on what needs to be thoroughly considered in advance of test.**
- **An example would be:**
 - **A high-speed logic string, such as a shift register, with inadequate output buffer performance that limits operation to 10% of the frequency capability.**
 - **In a case like this, the choice of output buffer type along with a concept such as a windowed shift register (WSR) approach [Berg, et al] would allow for a proper operation and data capture.**
 - **Of course, REAL logic rarely is just a string of shift registers and having appropriate designs within the FPGA that allow interpolation for applications is key (Berg, et al).**
- **Bottom line: know how the testing was done and the level of completeness and granularity of data captured.**



Tenet 3: The Analysis

- The real output of any SEE test campaign is not only the ability to determine rates for space usage, but also the *error signatures* of the events.
- This is the key to understanding the risk beyond the SEE rates and to provide the system designers the information to **properly design mitigation or fault tolerance approaches**.
- The simple way of viewing this is that all SEU events that cause SEFIs are not created equal:
 - They have different circuit responses. Thus, capturing and diagnosing the events can be a challenge.
 - One SEFI may change the operating mode, while another may cause a current increase.



Diatribes 2: Limiting cross-sections (1)

- The theory is pretty straightforward:
 - Just because an event is not observed during a SEE test run doesn't rule out the potential that the next particle will cause the event (or a different event).
- **SEE is known to be a Markov process** in that past performance is not necessarily an indicator what happens next.
 - One then assumes that the next particle will cause an event.
 - The *limiting cross-section* is usually designated as $1/(\text{fluence of the test run, i.e., the total number of particles/cm}^2 \text{ accumulated during that run})$.



Diatribes 2: Limiting cross-sections (2)

- A simple example was documented in 1998 by LaBel, et al for a memory device.
 - Proton SEE tests were performed with a sample size of 3 and a proton test fluence of 1×10^{10} p/cm²
 - A specific SEFI condition was not observed (row/column errors). However, it had been observed with heavy ions previously.
 - The project utilizing this device did not understand that this implied a *limiting cross-section*, as opposed to a zero cross-section or immunity to the effect.
 - They flew 1000 samples of this device and observed this SEFI in flight.
 - A re-test with 100 parts and a higher proton fluence confirmed this rare event and device sensitivity.

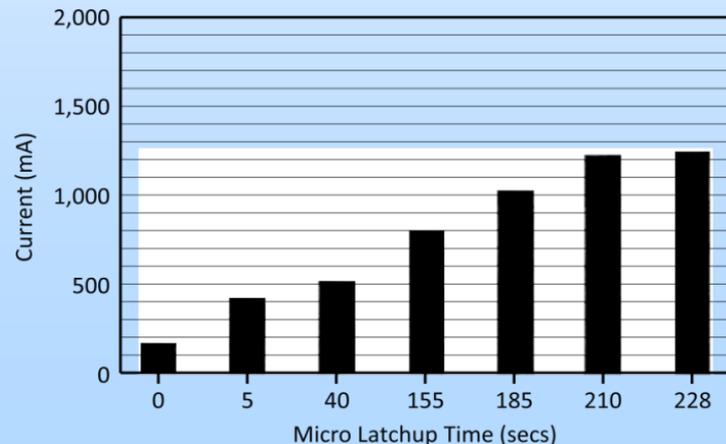
In cases of billion transistor FPGAs, the probability of stimulating all possible error signatures is statistically **zero** for a typical test campaign.

Thus, the best we can try to do is provide the limits for other error types not observed.



Caveat Emptor!

- The figure below is from the 1992 IEEE Radiation Effects Data Workshop (REDW) record (LaBel, et al.)
- To summarize what was presented,
 - A system level test of an INTEL 80386 processor and several peripherals was performed at Brookhaven National Laboratories (BNL) Single Event Upset Test Facility (SEUTF).
 - The data were for a representative test run and interpreted as “microlatchup” – a series of SEL events that caused a step-like increase with each event in the power supply current consumption.
 - However, the device continued to function during the test run even with the increases.





Mea Culpa!

- **Realistically, more diagnostics were needed to determine if these really were SEL events and not possibly caused by SEU hits to hidden logic or bus contention or another SEFI event.**
- **Even over twenty years ago, device complexity and understanding should have been better explored.**



Discussion

- **The realistic implications are different depending on whether the device is commercial-off-the-shelf (COTS) or custom-designed for radiation tolerance.**
 - **For COTS, you will be dealing with unknowns and limitations, hence, capturing as many error signatures as possible provides the most useful information.**
 - **It's what the designers need to build appropriate mitigation into their systems.**
 - **For custom design, you should be able to predict error signatures as long as there aren't intellectual property (IP) blocks of unknown designs (black box).**
 - **Thus, tests here are usually more about statistics to meet SEU rates or threshold levels.**
 - **That is, unless unexpected SEFI events occur.**
- **Devices like FPGAs are afflicted with both implications:**
 - **Custom designs are created, but there's also manufacturer-embedded IP and hidden functions that require detailed error signature capture.**
 - ***Double the challenge!***



Summary

- While far from a complete treatise on FPGA SEE testing, we have provided some caveats in reviewing a FPGA's SEE performance based on collected data.
- The level of understanding of the device's internal workings as well as the limitations of the test setup, allow proper risk-based analyses to be performed on the collected SEE data.
 - *It's not just event rates, but event signatures and interpretation!*



Acknowledgements

- **We would like to thank the support of the NASA Electronic Parts and Packaging Program (NEPP).**
- **The authors would also like to thank Martha O'Bryan for her aid in putting this presentation together.**