Electrical, Electronic and Electromechanical (EEE) Parts in the New Space Paradigm: *When is Better the Enemy of Good Enough?*

Kenneth A. LaBel
ken.label@nasa.gov
301-286-9936

Michael J. Sampson
michael.j.sampson@nasa.gov
301-614-6233

Co- Managers, NEPP Program
NASA/GSFC
http://nepp.nasa.gov

Unclassified

To be presented by Kenneth A. LaBel at 2016 SERESSA 12th International School on the Effects of Radiation on Embedded Systems for Space Applications, Montreal, Canada, November 7-10, 2016.

Acronyms

Acronym	Definition
COTS	Commercial off the Shelf
EDAC	Error Detection and Correction
EEE	Electrical, Electronic, and Electromechanical
I/O	Input/Output Operating System
LEO	Low Earth Orbit
POF	Physics of Failure
Rad Hard	Radiation Hardened
SOC	System on a Chip
SwaP	Size, Weight, and Power
TID	Total Ionizing Dose

Abstract

- As the space business rapidly evolves to accommodate a lower cost model of development and operation via concepts such as commercial space and small spacecraft (aka, CubeSats), traditional EEE parts screening and qualification methods are being scrutinized under a risk-reward trade space. In this presentation, two basic concepts will be discussed:
  - The movement from complete risk aversion EEE parts methods to managing and/or accepting risk via alternate approaches; and,
  - A discussion of “over-design” focusing on both electrical design performance and bounding margins.
- Example scenarios will be described as well as consideration for trading traditional versus alternate methods.

Outline

- The Changing Space Market
  - Commercial Space and "Small" Space
- EEE Parts Assurance
- Modern Electronics
  - Magpie Syndrome
- Breaking Tradition: Alternate Approaches
  - Higher Assembly Level Tests
  - Use of Fault Tolerance
- Mission Risk and EEE Parts
- Summary

Hubble Space Telescope courtesy NASA

Space Missions:
How Our Frontiers Have Changed

- **Cost constraints and cost "effectiveness" have led to dramatic shifts away from traditional large-scale missions (ex., Hubble Space Telescope).**
- **Two prime trends have surfaced:**
  – **Commercial space ventures where the procuring agent "buys" a service or data product and the implementer is responsible for ensuring mission success with limited agent oversight. And,**
  – **Small missions such as CubeSats that are allowed to take higher risks based on mission purpose and cost.**
- **These trends are driving the usage of non Mil/Aero parts such as Automotive grade (see Mike Sampson's talk) and "architectural reliability" approaches.**

EEE Parts Assurance

Assurance for EEE Parts

- ***Assurance*** **is**
  - **Knowledge of**
    - **The supply chain and manufacturer of the product,**
    - **The manufacturing process and its controls, and,**
    - **The physics of failure (POF) related to the technology.**
  - **Statistical process and inspection via**
    - **Testing, inspection, physical analyses and modeling.**
  - **Understanding the application and environmental conditions for device usage.**
    - **This includes:**
      - **Radiation,**
      - **Lifetime,**
      - **Temperature,**
      - **Vacuum, etc., as well as,**
      - **Device application and appropriate derating criteria.**

Reliability and Availability

- **Reliability (Wikipedia)**
  - **The ability of a system or component to perform its required functions under stated conditions for a specified period of time.**
    - **Will it work for as long as you need?**
- **Availability (Wikipedia)**
  - **The degree to which a system, subsystem, or equipment is in a specified operable and committable state at the start of a mission, when the mission is called for at an unknown, *i.e.,* a random, time. Simply put, availability is the proportion of time a system is in a functioning condition. This is often described as a mission capable rate.**
    - **Will it be available when you need it to work?**
- **Combining the two drives mission requirements:**
  - ***Will it work for as long as and when you need it to?***

What does this mean for EEE parts?

- The more *understanding* you have of a device's failure modes and causes, the higher the *confidence* level that it will perform under mission environments and lifetime
  - *High confidence* = "it has to work"
    - High confidence in both reliability and availability.
  - *Less confidence* = "it may to work"
    - Less confidence in both reliability and availability.
    - It may work, but prior to flight there is less certainty.

Traditional Approach to Confidence

- **Part level qualification**
  - **Qualification processes are designed to statistically understand/remove known reliability risks and uncover other unknown risks inherent in a part.**
    - **Requires significant sample size and comprehensive suite of piecepart testing (insight) – *high confidence method***
- **Part level screening**
  - **Electronic component screening uses environmental stressing and electrical testing to identify marginal and defective components within a procured lot of EEE parts.**

However, tradition doesn't match the changing space market and alternate EEE parts approaches that may be

"good enough"

are being used.

(Discussed later in presentation.)

Modern Electronics

The Magpie Syndrome:
The Electrical Designer's Dilemma

- Magpie's are known for being attracted to bright, shiny things.
- In many ways, the modern electrical engineer is a Magpie:
  - They are attracted to the latest state-of-the-art devices and EEE parts technologies.
    - These can be any grade of EEE parts that aren't qualified for space nor radiation hardened.
  - These bright and shiny parts may have very attractive performance features that aren't available in higher-reliability parts:
    - Size, weight, and power (SwaP),
    - Integrated functionality,
    - Speed of data collection/transfer,
    - Processing capability, etc…

When Should a Magpie Fly?

- **While not designed for usage in the harsh environs of space, there are still multiple scenarios where usage of Magpies may be considered:**
  - **Mil/Aero alternatives are not available,**
    - **Ex., SWaP or functionality or procurement schedule,**
  - **A mission has a relatively short lifetime or benign space environment exposure,**
    - **Ex., 6 month CubeSat mission in LEO,**
  - **A system can assume possible unknown risks,**
    - **Ex., technology demonstration mission,**
  - **Device upscreening (per mission requirements) and system validation are performed to obtain confidence in usage,**
  - **System level assurances based on fault tolerance and higher assembly level test and validation are deemed sufficient.**
    - **This is a systems engineering trade that takes a multi-disciplinary review.**
  - **Or maybe as a pathfinder for future usage.**
    - **Out of scope for this talk: use of flight data for "qualification".**

Magpie Constraints

- **But Magpies aren't designed for space flight (just some aviary aviation at best)!**
- **Sample differences include:**
  - **Temperature ranges,**
  - **Vacuum performance,**
  - **Shock and vibration,**
  - **Lifetime, and**
  - **Radiation tolerance.**
- **Traditionally, "upscreening" at the part level has occurred.**
  - **Definition: A means of assessing a portion of the inherent reliability of a device via test and analysis.**
    - **Note: Discovery of a upscreened part failure occurs regularly.**
- **The following charts discuss alternate approaches.**

Breaking Tradition: Alternate Approaches

Assembly Testing:
Can it Replace Testing at the Parts Level?

We can test devices,

but how do we test systems?

Or better yet, systems of systems on a chip (SOC)?

Not All Assemblies are Equal

- **Consider assemblies having two distinct categories**
  - **Off the shelf (you get what you get) such as COTS, and,**
  - **Custom (possibility of having "design for test" included")**
    - **Still won't be as complete as single part level testing, but it does reduce some challenges.**
- **For COTS assemblies, some of the specific concerns are:**
  - **Bill-of-materials may not include lot date codes or device manufacturer information.**
  - **Individual part application may not be known or datasheet unavailable.**
  - **The possible variances for "copies" of the "same" assembly:**
    - **Form, fit, and function EEE parts may mean various manufacturers, or,**
    - **Lot-to-lot and even device-to-device differences in reliability/availability.**

Sample Challenges for Testing Assemblies

- Limited statistics versus part level approaches due to sample size.
- Inspection constraints.
- Acceleration factors
  - Temperature testing limited to “weakest” part.
  - Voltage testing may be limited by on-board/on-chip power regulation.
- Limited test points and I/O challenge adequate stress data capture.
- Ensuring adequate fault coverage testing.
- Visibility of errors/failures/faults due to limited I/O availability.
- System operation.
  - Ex., Using nominal flight software versus a high stress test approach.
- Error propagation
  - An error occurs but does not propagate outward until some time later due to system operations such as those of an interrupt register.
- Fault masking during radiation exposure
  - Too high a particle rate or too many devices being exposed simultaneously.

Using Fault Tolerance

- **Making a system more "reliable/available" can occur at many levels**
  - **Operational**
    - **Ex., no operation in the South Atlantic Anomaly (proton hazard)**
  - **System**
    - **Ex., redundant boxes/busses or swarms of nanosats**
  - **Circuit/software**
    - **Ex., error detection and correction (EDAC) scrubbing of memory devices by an external device or processor**
  - **Device (part)**
    - **Ex., triple-modular redundancy (TMR) of internal logic within the device**
  - **Transistor**
    - **Ex., use of annular transistors for TID improvement**
  - **Material**
    - **Ex., addition of an epi substrate to reduce SEE charge collection (or other substrate engineering)**

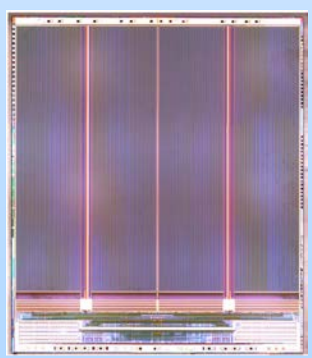
Good engineers can invent infinite solutions,
but the solution used must be adequately validated.

Example:

Is Radiation Testing Always Required for COTS?

- **Exceptions for testing may include**
  - **Operational**
    - **Ex., The device is only powered on once per orbit and the sensitive time window for a single event effect is minimal**
  - **Acceptable data loss**
    - **Ex., System level error rate (availability) may be set such that data is gathered 95% of the time.**
      - **Given physical device volume and assuming every ion causes an upset, this worst-case rate may be tractable.**
  - **Negligible effect**
    - **Ex., A 2 week mission on a shuttle may have a very low Total Ionizing Dose (TID) requirement.**

Memory picture courtesy NASA/GSFC, Code 561



A flash memory may be acceptable without testing if a low TID requirement exists or not powered on for the large majority of time.

Is knowledge of EEE Parts Failure Modes Required To Build a Fault Tolerant System?

- **The system *may* work, but do we have adequate confidence in the system to have adequate reliability and availability prior to launch?**
  - **What are the "unknown unknowns"?**
    - **Can we account for them?**
  - **How do you calculate risk with unscreened/untested EEE parts?**
  - **Do you have a common mode failure potential in your design?**
    - **I.e., a design with identical redundant strings rather than having independent redundant strings.**
  - **How do you adequately validate a fault tolerant system for space?**
    - ***This is a critical point.***

Bottom Line on Assembly Testing and Fault Tolerance

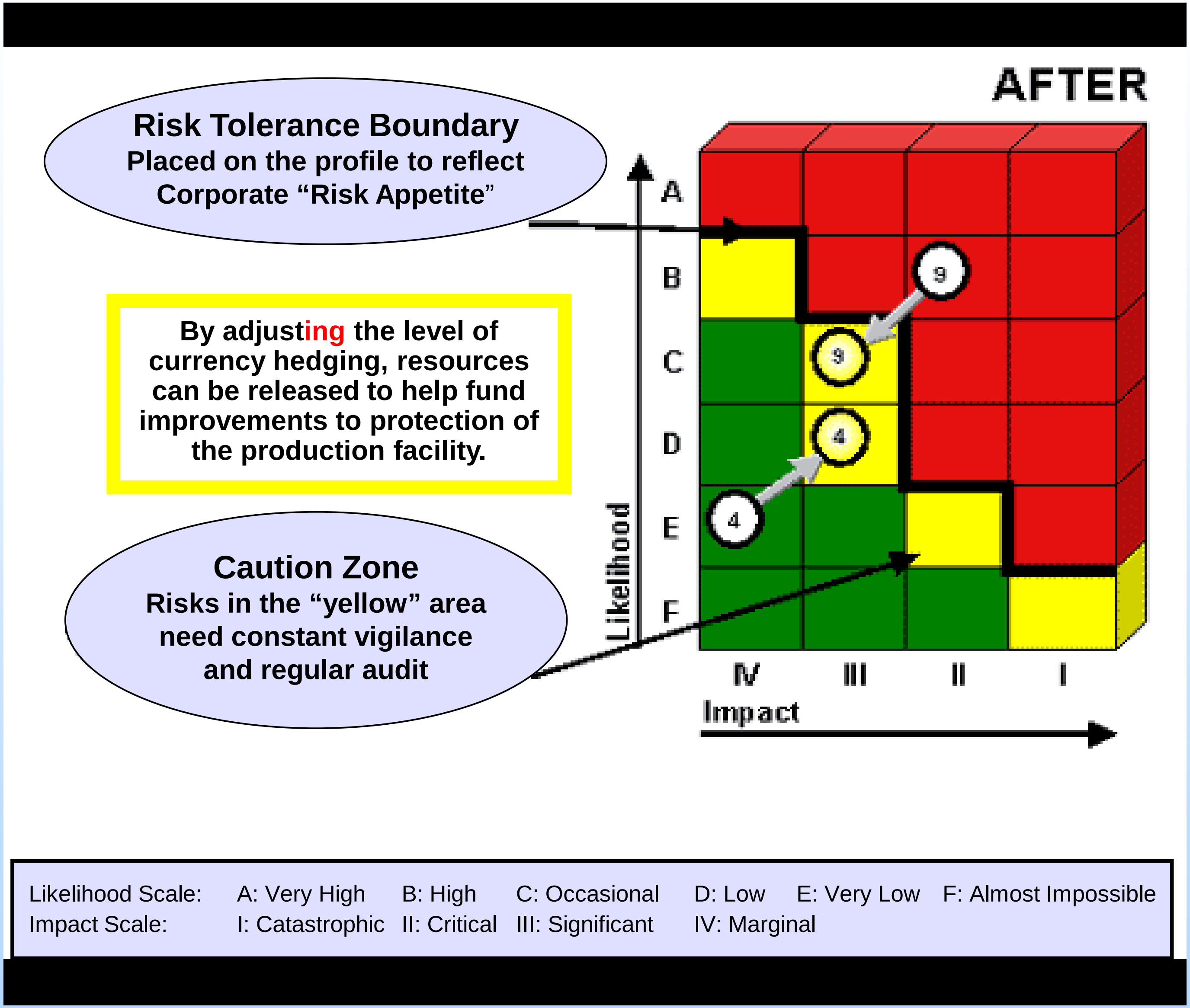
- **While clearly ANY testing is better than none, assembly testing has limitations compared to the individual EEE part level.**
  - **This is a risk-trade that's still to be understood.**
  - **No *definitive* study exists comparing this approach versus traditional parts qualification and screening.**
- **Fault tolerance needs to be validated.**
  - **Understanding the fault and failure signatures is required to design appropriate tolerance.**
  - **The more complex the system, the harder the validation is.**

Mission Risk and EEE Parts

Understanding Risk

- **The risk management requirements may be broken into three considerations**
  - **Technical/Design – "The Good"**
    - **Relate to the circuit designs not being able to meet mission criteria such as jitter related to a long dwell time of a telescope on an object**
  - **Programmatic – "The Bad"**
    - **Relate to a mission missing a launch window or exceeding a budgetary cost cap which can lead to mission cancellation**
  - **Radiation/Reliability – "The Ugly"**
    - **Relate to mission meeting its lifetime and performance goals without premature failures or unexpected anomalies**
- ***Each mission must determine its priorities among the three risk types***

Background: Traditional Risk Matrix



Space Missions: EEE Parts and Risk

- **The determination of acceptability for device usage is a complex trade space.**
  - **Every engineer will "solve" a problem differently:**
    - **Ex., software versus hardware solutions.**
- **The following chart proposes an alternate mission risk matrix approach for EEE parts based on:**
  - **Environment exposure,**
  - **Mission lifetime, and,**
  - **Criticality of implemented function.**
- **Notes:**
  - **"COTS" implies any grade that is not space qualified and radiation hardened.**
  - **Level 1 and 2 refer to traditional space qualified EEE parts.**

Notional EEE Parts Selection Factors

Criticality

High	Level 1 or 2 suggested. COTS upscreening/ testing recommended. Fault tolerant designs for COTS.	Level 1 or 2, rad hard suggested. Full upscreening for COTS. Fault tolerant designs for COTS.	Level 1 or 2, rad hard recommended. Full upscreening for COTS. Fault tolerant designs for COTS.
Medium	COTS upscreening/ testing recommended. Fault-tolerance suggested	COTS upscreening/ testing recommended. Fault-tolerance recommended	Level 1 or 2, rad hard suggested. Full upscreening for COTS. Fault tolerant designs for COTS.
Low	COTS upscreening/ testing optional. Do no harm (to others)	COTS upscreening/ testing recommended. Fault-tolerance suggested. Do no harm (to others)	Rad hard suggested. COTS upscreening/ testing recommended. Fault tolerance recommended
	Low	Medium	High

Environment/Lifetime

A Few Details on the "Matrix"

- **When to test:**
  - **"Optional"**
    - **Implies that you might get away without this, but there's residual risk.**
  - **"Suggested"**
    - **Implies that it is good idea to do this, and likely some risk if you don't.**
  - **"Recommended"**
    - **Implies that this really should be done or you'll definitely have some risk.**
  - **Where just the item is listed (like "full upscreening for COTS")**
    - **This should be done to meet the criticality and environment/lifetime concerns.**
- **The higher the level of risk acceptance by a mission, the higher the consideration for performing alternate assembly level testing versus traditional part level.**
- **All fault tolerance must be validated.**

Good mission planning identifies where on the matrix a EEE part lies.

Summary

- **In this talk, we have presented:**
  - **An overview of considerations for alternate EEE parts approaches:**
    - **Technical, programmatic, and risk-oriented**
      - **Every mission views the relative priorities differently.**
- **As seen below, every decision type may have a process.**
  - **It's all in developing an appropriate one for your application and avoiding "buyer's remorse"!**