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

Presented by Kenneth A. LaBel at SERESSA 2017 the 13th International School on the Effects of Radiation on Embedded Systems for Space Applications, Munich (Garching), Germany, October 23-26, 2017.

Acronyms

Acronym	Definition
ADC	Analog to Digital Converter
AES	Advanced Encryption Standard
AF	Air Force
AMS	Agile Mixed Signal
ARC	Ames Research Center
ARM	ARM Holdings Public Limited Company
Bayes Net	Bayesian Networks
BN	Bayesian Networks
CAN	Controller Area Network
CAN-FD	Controller Area Network Flexible Data-Rate
CCI	Cache coherent interconnect
Codec	a device or program that compresses data to enable faster transmission and decompresses received data
COF	chemistry of failure
COTS	Commercial Off The Shelf
CRC	Cyclic Redundancy Check
CSE	Communications Security Establishment
CSI2	Camera Serial Interface 2nd Generation
CU	Control Unit
DCU	Display Control Unit
DDR	Double Data Rate (DDR3 = Generation 3; DDR4 = Generation 4)
DEBUG	identify and remove errors from (computer hardware or software)
DMA	Direct Memory Access
DOA	dead on arrival
DSP	Digital Signal Processing
dSPI	Dynamic Signal Processing Instrument
Dual Ch.	Dual Channel
ECC	Error-Correcting Code
EDAC	error detection and correction
EEE	Electrical, Electronic, and Electromechanical
EMAC	Equipment Monitor And Control
epi	Epitaxy, the deposition of a crystalline overlayer on a crystalline substrate
ESD	electrostatic discharge
eTimers	Event Timers
FCCU	Fluidized Catalytic Cracking Unit
FlexRay	FlexRay Communication Controller
Gb	Gigabyte
GIC	Global Industry Classification
Gov't	Government
GPU	Graphics Processing Unit
GSFC	Goddard Space Flight Center
GSN	Goal Structuring Notation
GTH/GTY	Transceiver Type
HDIO	High Density Digital Input/Output
HDR	High-Dynamic-Range
HPIO	High Performance Input/Output
I/O	input/output

Acronym	Definition
I2C	Inter-Integrated Circuit
JPEG	Joint Photographic Experts Group
JPL	NASA Jet Propulsion Laboratory
L2 Cache	independent caches organized as a hierarchy (L1, L2, etc.)
LEO	low earth orbit
LinFlex	Local Interconnect Network Flexible
L-mem	Long-Memory
LP	Low Power
M/L BIST	Memory/Logic Built-In Self-Test
MAIW	Mission Assurance Improvement Workshop
MBMA	model based mission assurance
MBSE	Model-Based Systems Engineering
MIPI	Mobile Industry Processor Interface
NAND	Negated AND or NOT AND
NASA	National Aeronautics and Space Administration
NEPP	NASA Electronic Parts and Packaging
NOR	Not OR logic gate
OCM	on-chip RAM
PCIe	Peripheral Component Interconnect Express
PCIe Gen2	Peripheral Component Interconnect Express Generation 2
POF	Physics of Failure
PS-GTR	PS-GTR is a type of transceiver
R&D	Research and Development
Rad Hard	radiation hardened
RAM	Random Access Memory
RGB	Red, Green, and Blue
RH	Radiation Hardened
RHA	Radiation Hardeness Assurance
SAR	Successive-Approximation-Register
SATA	Serial Advanced Technology Attachment
SCU	Secondary Control Unit
SD/eMMC	Secure Digital embedded MultiMediaCard
SD-HC	Secure Digital High Capacity
SEE	Single Event Effect
SMMU	System Memory Management Unit
SOC	Systems on a Chip
SPI	Serial Peripheral Interface
SwaP	Size, weight, and power
SysML	System Modeling Language
TCM	tightly-coupled memory
TID	Total Ionizing Dose
TMR	triple-modular redundancy
T-Sensor	Temperature-Sensor
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
WDT	watchdog timer
Zipwire	Freescale Zipwire interface

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 and swarms), 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 emerging assurance methods to reduce overdesign as well emerging model based mission assurance (MBMA) concepts.
- Example scenarios will be described as well as consideration for trading traditional versus alternate methods.

Outline

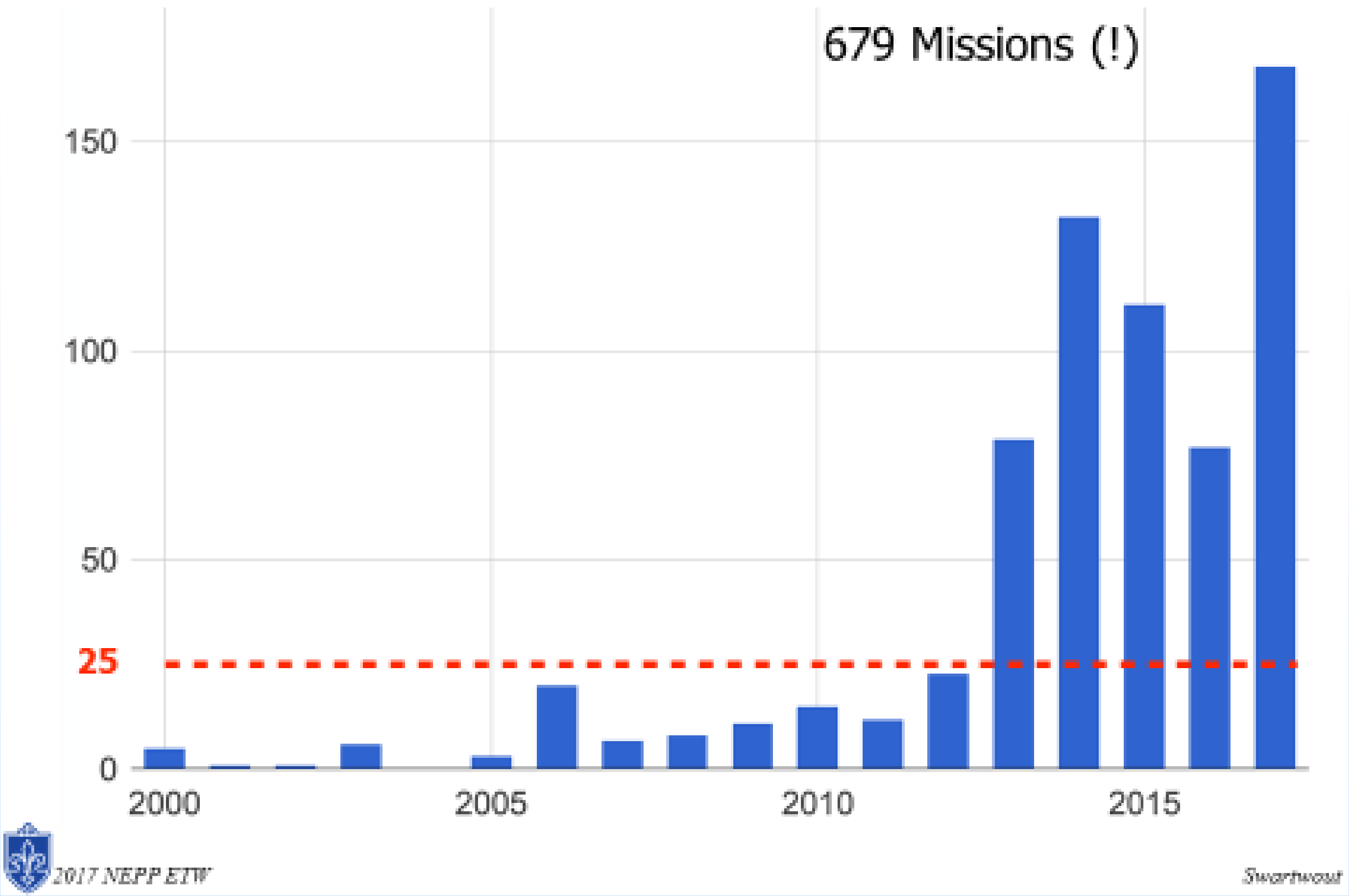
- The Changing Space Market
  - Commercial Space and "Small" Space
- EEE Parts Assurance
- Modern Electronics
  - Magpie Syndrome
- Breaking Tradition: Alternate Approaches
  - Higher Assembly Level Tests
  - Use of Fault Tolerance
- Mission Risk and EEE Parts
- Summary

Hubble Space Telescope courtesy NASA

Space Missions:
How Our Frontiers Have Changed

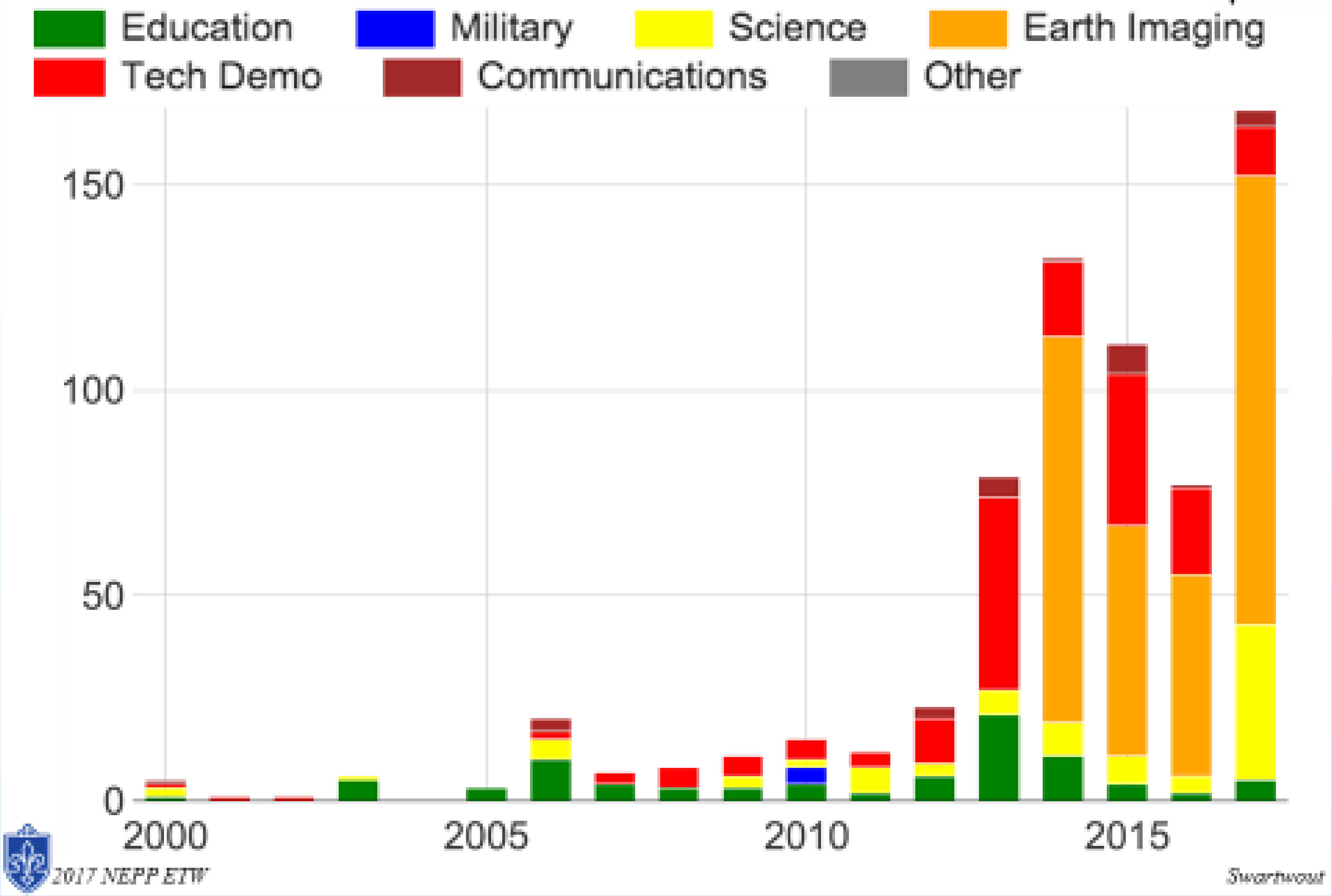
- **Cost constraints and cost "effectiveness" have led to dramatic shifts away from traditional large-scale missions (ex., Hubble Space Telescope).**
- **Two prime trends have surfaced:**
  - **Commercial space ventures where the procuring agent "buys" a service or data product and the implementer is 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 and "architectural reliability" (aka, resilience) approaches.**

CubeSats Launched (2000-2017)



Michael Swartwout, "CubeSat Mission Success: 2017 Update (with a closer look at the effect of process management on outcome)," NASA Electronic Parts and Packaging (NEPP) Program, 2017 NEPP Electronics Technology Workshop, June 26-29, 2017.

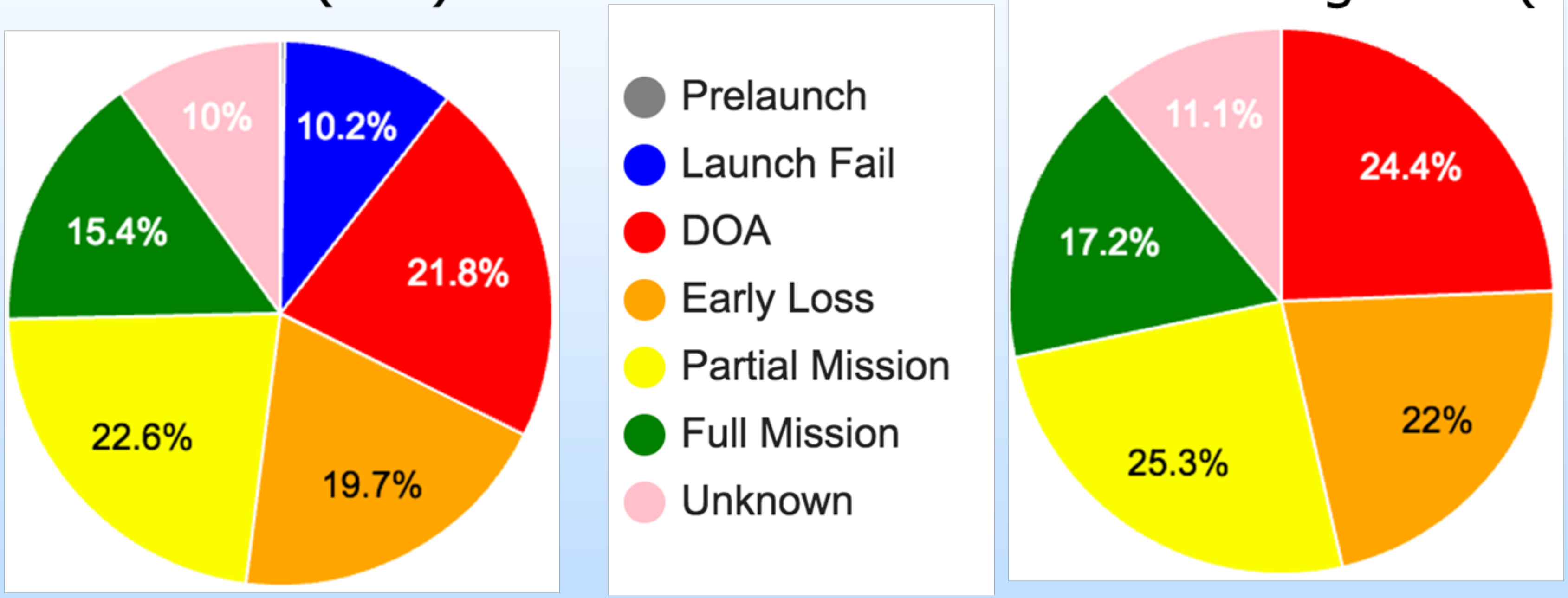
CubeSat by Mission Type



Michael Swartwout, "CubeSat Mission Success: 2017 Update (with a closer look at the effect of process management on outcome)," NASA Electronic Parts and Packaging (NEPP) Program, 2017 NEPP Electronics Technology Workshop, June 26-29, 2017.

All Missions (371)

All missions reaching orbit (332)



Michael Swartwout, "CubeSat Mission Success: 2017 Update (with a closer look at the effect of process management on outcome)," NASA Electronic Parts and Packaging (NEPP) Program, 2017 NEPP Electronics Technology Workshop, June 26-29, 2017.

EEE Parts Assurance

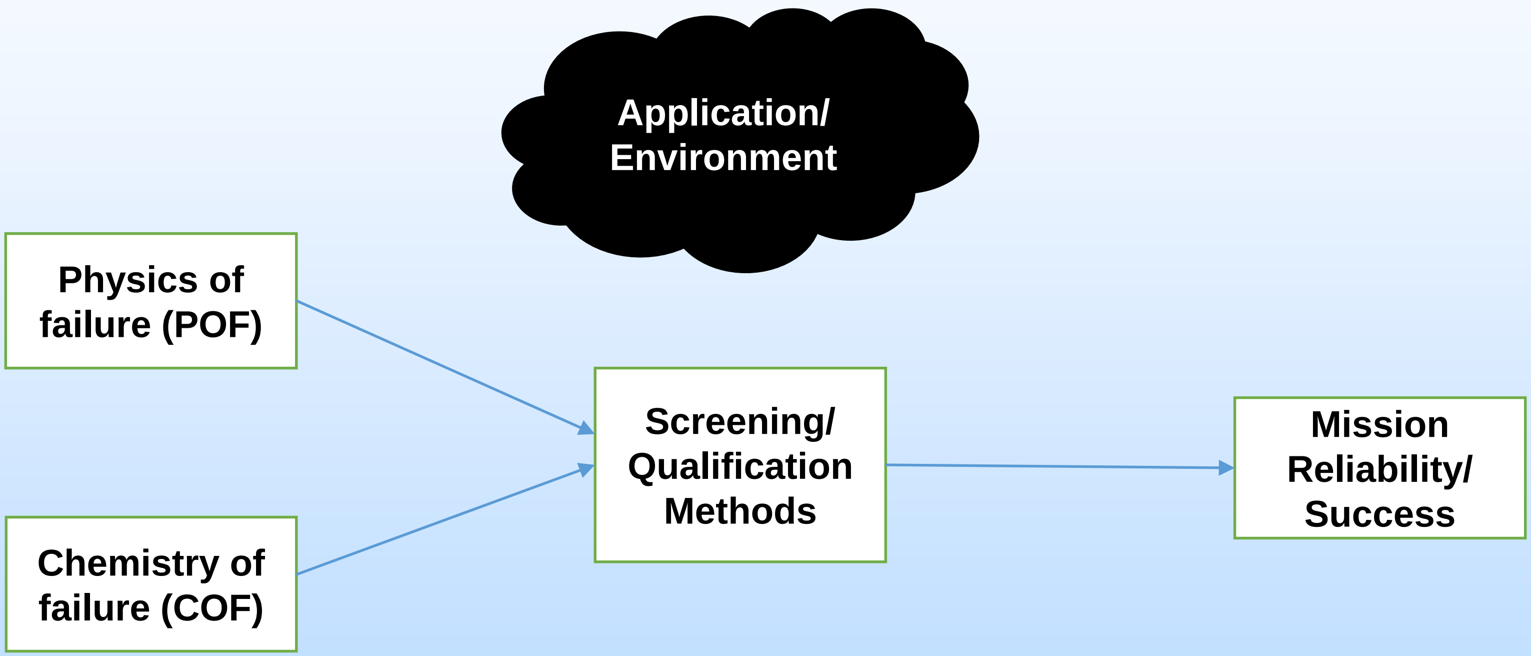
Assurance for EEE Parts

- ***Assurance*** **is knowledge of**
  - **The supply chain and manufacturer of the product**
  - **The manufacturing process and its controls**
  - **The physics of failure (POF) and chemistry of failure (COF) related to the technology.**
  - **Statistical process and inspection via**
    - **Testing, inspection, physical analyses and modeling.**
      - **Audits, process data analysis, electrostatic discharge (ESD), …**
  - **Test/Qualification/Screening methods**

– **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.**

Taking a Step Back…



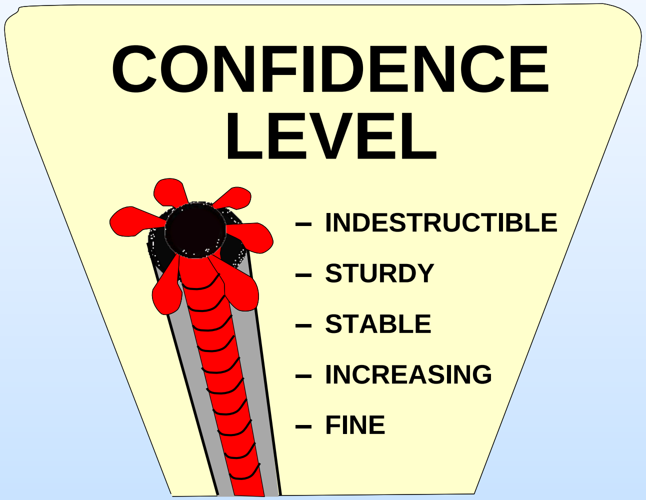
It's not just the technology, but how to view the need for safe insertion into space programs.

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 EEE Parts Approach to *Confidence*

- **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.**
- **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***

However, tradition doesn't match the changing space market.

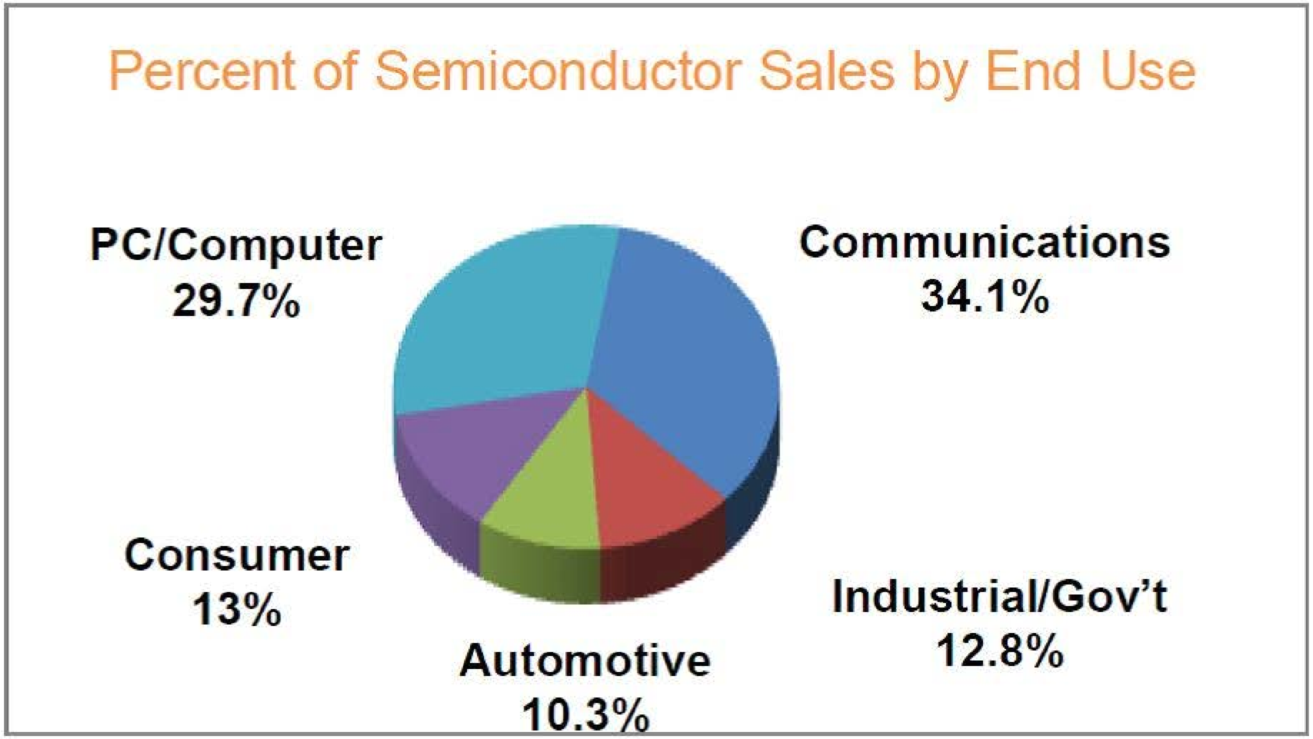
Alternate EEE parts approaches that may be "good enough" are being used.

(Discussed later in presentation.)

Modern Electronics

A History Lesson

2015 Global Semiconductor Market: $335 Billion



Source: WSTS End Use Report, 2015
Note: Military is <1% and is included in Industrial/Gov't

Military and Aerospace share is estimated at ~$3.1B in 2015.

Aerospace is a small percentage of this amount.

For comparison, in 1975

the Military and Aerospace market share was ~$50%!

EEE parts are available in "grades"

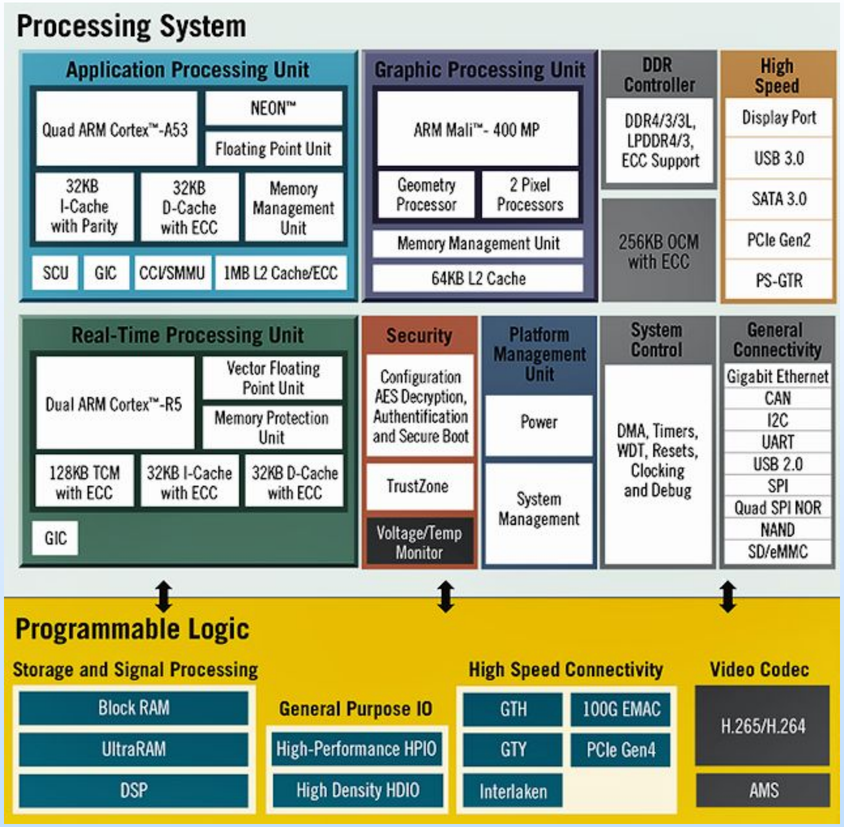
- **Grades – Designed, certified, qualified, and/or tested for specific environmental characteristics.**
  - **E.g., Operating temperature range, vacuum, radiation, exposure,…**
- **Examples: Aerospace, Military, Space Enhanced Product, Enhanced Product, Automotive, Medical, Extended-Temperature-Commercial, and Commercial.**
  - **Aerospace Grade is the traditional choice for space usage, but has relatively few available parts and their performance lags behind commercial counterparts (speed, power).**
    - **Designed and tested for radiation and reliability for space usage.**
- **NASA uses a wide range of EEE part grades depending on many factors (technical, programmatic, and risk).**

The Magpie Syndrome:
The Electrical Designer's Dilemma

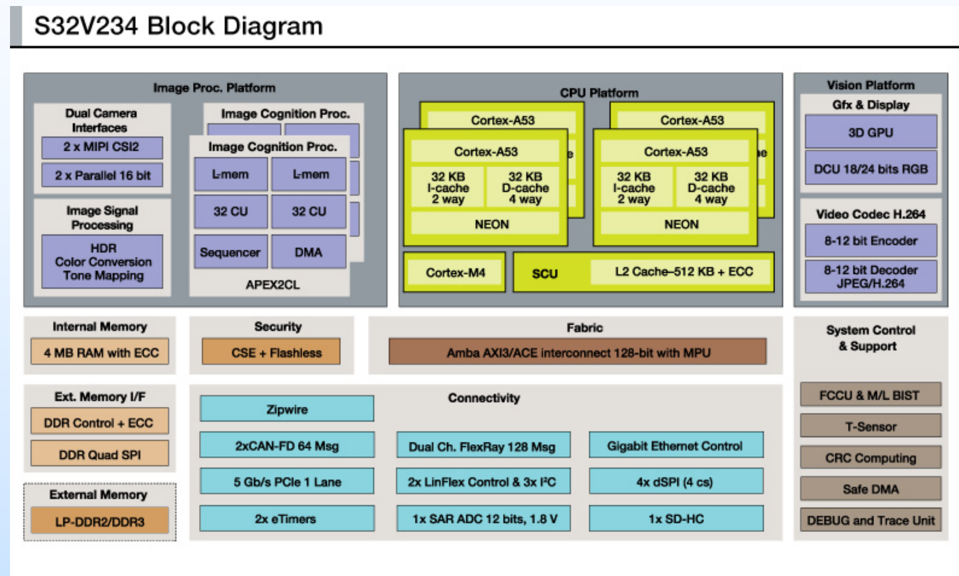
- **Magpie's are known for being attracted to bright, shiny things.**
- **In many ways, the modern electrical engineer is a Magpie:**
  - ***They are attracted to the latest state-of-the-art devices and EEE parts technologies.***
    - **Usually any grade of EEE parts that aren't qualified for space 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…**

Graphic from Clip Arts Free net.

Example Magpie EEE Parts

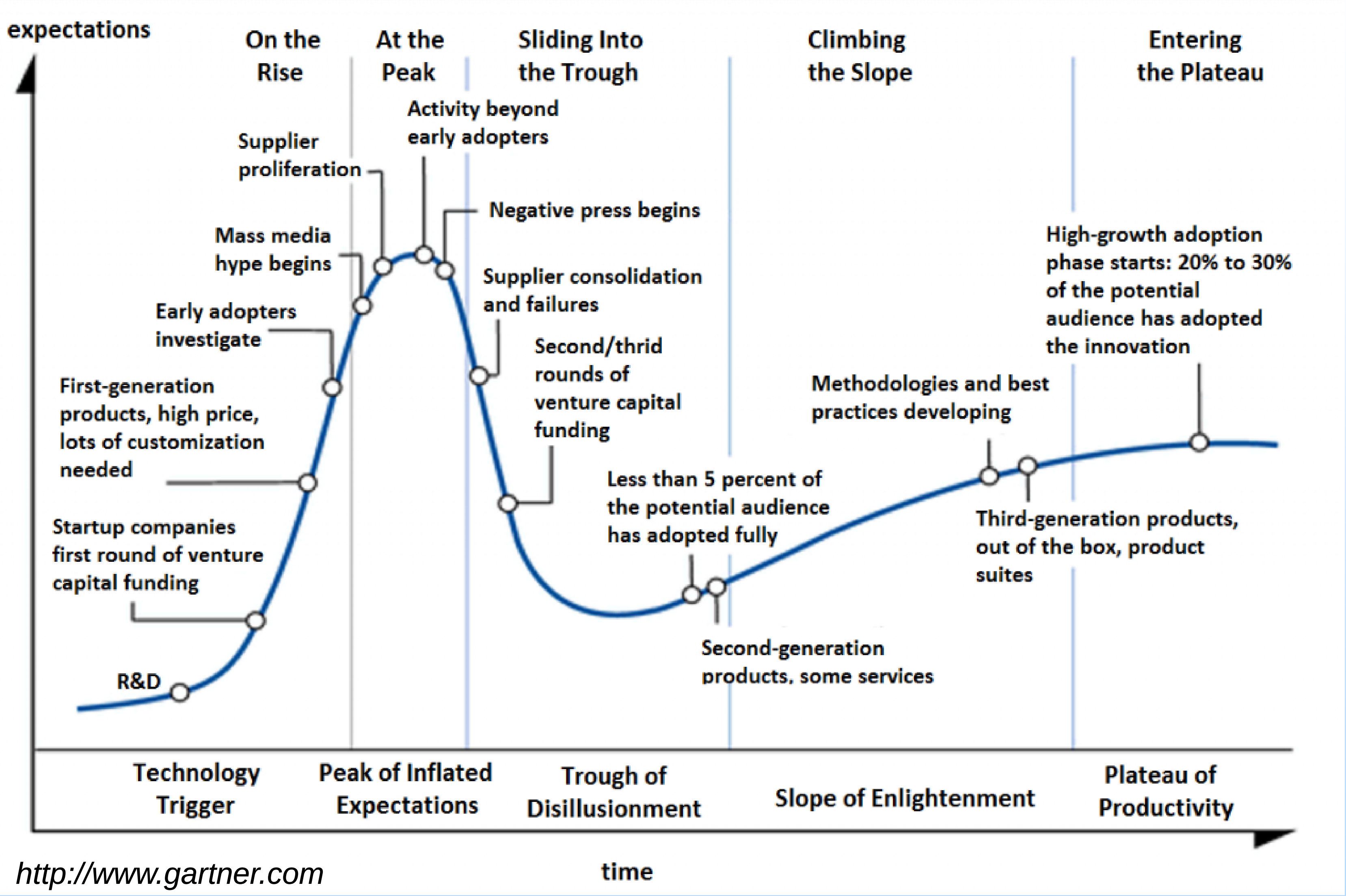


Xilinx Zynq UltraScale+
Multi-Processor System on a Chip (MPSoC) -
16nm CMOS with Vertical FinFETS
Xilinx.com



Advanced Driver Assistance System (ADAS)
Sensor Fusion Processor
Freescale.com

Gartner Hype Cycle –
Reality of Shiny New Things



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.

Graphic from Free Vector Art.

- 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.
    - It's not increasing reliability!
  - Note: Discovery of a upscreened part failure occurs regularly.

When Should a Magpie Fly?

- 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., 3 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, higher assembly level test, and adequate validation are deemed sufficient.
  - This is a systems engineering trade that takes a multi-disciplinary review.
- As a pathfinder for future usage.
  - Out of scope for this talk: use of flight data for "qualification".

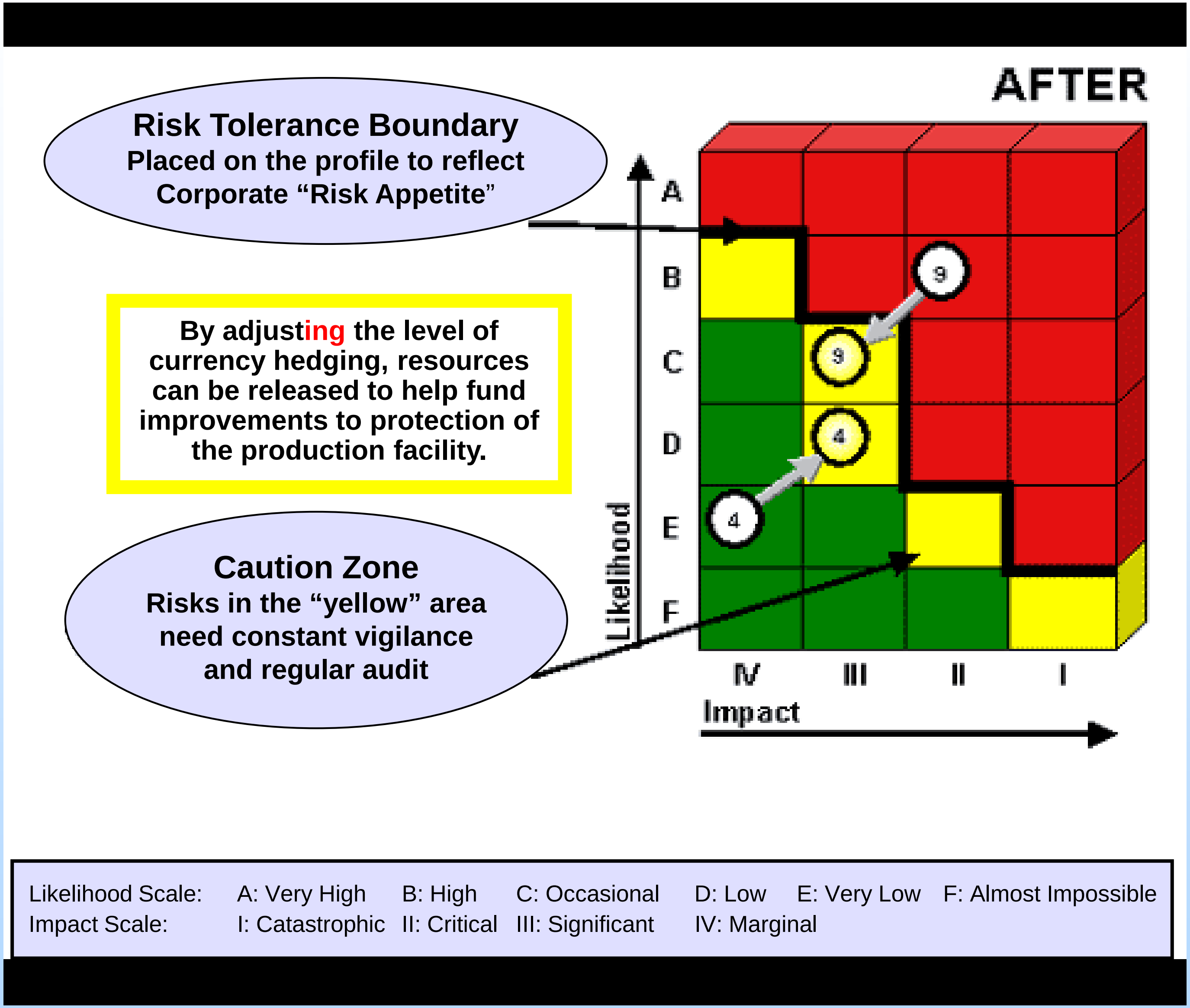
Mission Risk and EEE Parts

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***

Graphic from Free Vector Art.

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"

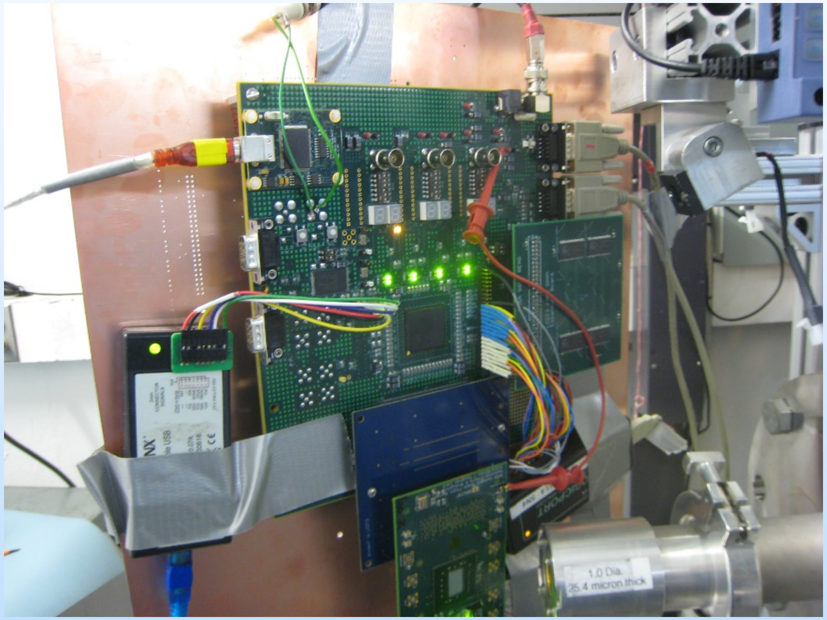
- When to test:
  - "Optional"
    - Implies that you might get away without this, but there's residual risk.
  - "Suggested"
    - Implies that it is good idea to do this, and likely some risk if you don't.
  - "Recommended"
    - Implies that this really should be done or you'll definitely have some 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.

Breaking Tradition:

Alternate Approaches to EEE Parts Assurance

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



NASA GSFC Picture of FPGA tester.

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 two distinct categories of assemblies:
  - Off the shelf (you get what you get) such as COTS, and,
  - Custom (possibility of having specific “design for test”)
    - Still won’t be as complete as single part level testing, but it does reduce some challenges.
- For COTS assemblies, some specific concerns include:
  - 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.**
- **Reliability 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 = inadequate visibility of errors/failures/faults.**
- **Inadequate fault coverage testing.**
- **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 to Improve "Reliability/Availability"

- **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 Total Ionizing Dose (TID) improvement**
- **Material**
  - **Ex., addition of an epi substrate to reduce Single Event Effect (SEE) charge collection (or other substrate engineering)**

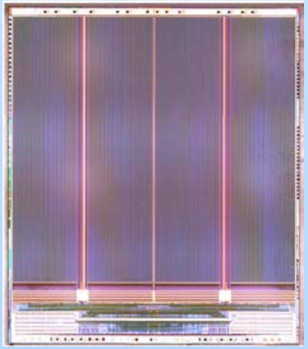
Good engineers can invent infinite solutions, but the solution used must be adequately validated.

It's easy to show a working block diagram, it's hard to provide sufficient validation details.

Possible Exceptions:
Is Radiation Testing Always Required for COTS?

- **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 space station may have a very low Total Ionizing Dose (TID) requirement.

Memory picture courtesy NASA/GSFC, Code 561



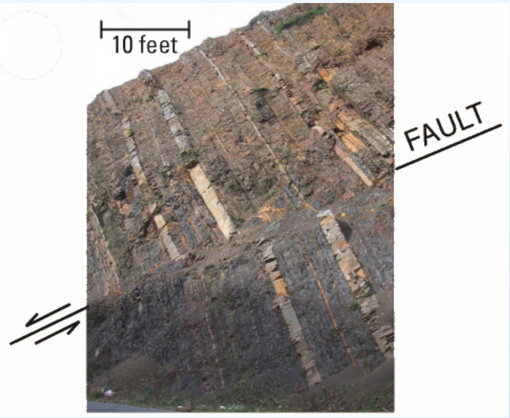
A flash memory may be acceptable without testing if a low TID requirement exists or not powered on for the large majority of time.

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

- **The system *may* work, but is there adequate confidence in the system to meet reliability and availability after launch?**
- **In no particular order:**
  - **What are the "unknown unknowns"?**
    - **Can we account for them?**
  - **How do you adequately validate a fault tolerant system for space?**
    - ***This is a critical point.***
  - **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.**

Bottom Line on Assembly Testing and Fault Tolerance

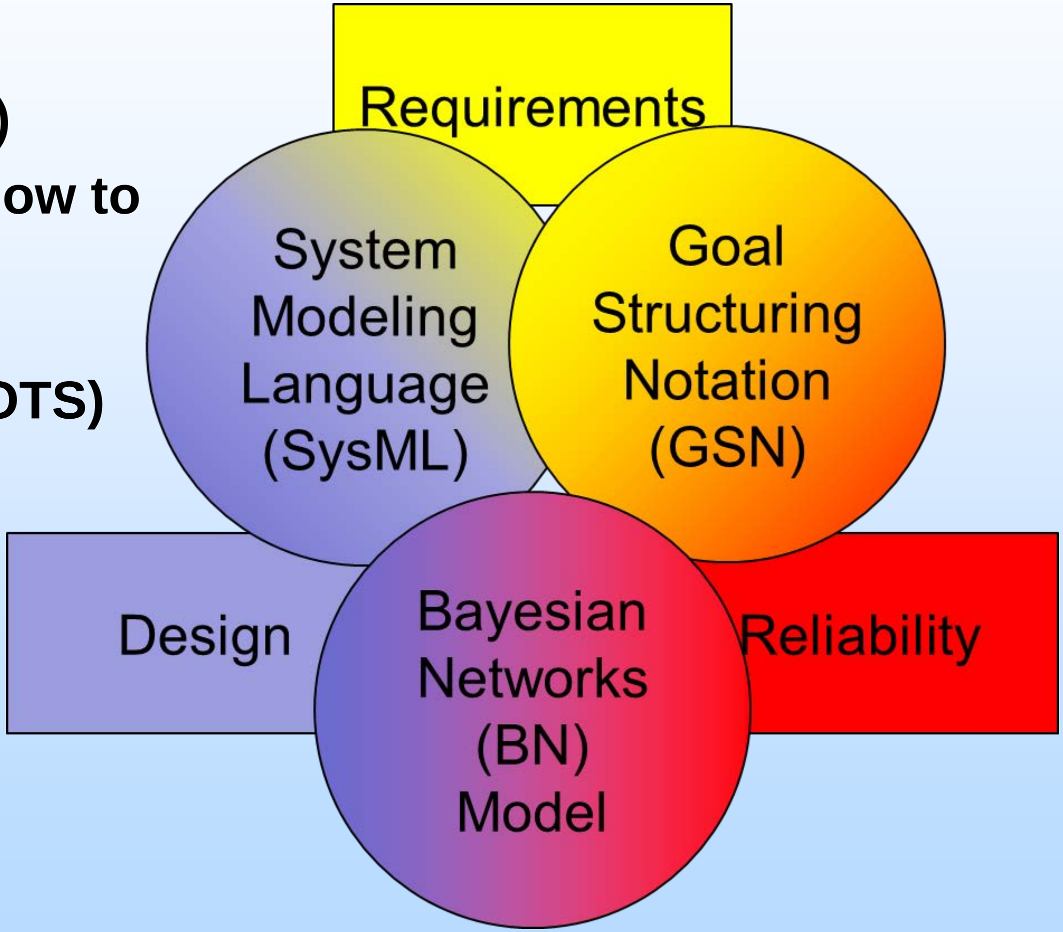
- **While clearly ANY testing is better than none, assembly testing has limitations compared to the individual EEE part level.**
  - **This is a risk-trade that's still to be understood.**
  - **No *definitive* study exists comparing this approach versus traditional parts qualification and screening.**



- **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.**

Model Based Mission Assurance (MBMA)

- Motivation
  - Commercial parts (COTS)
  - Document-centric work flow to model-based system engineering
  - System mitigation (for COTS)
  - Single source of system design parameters

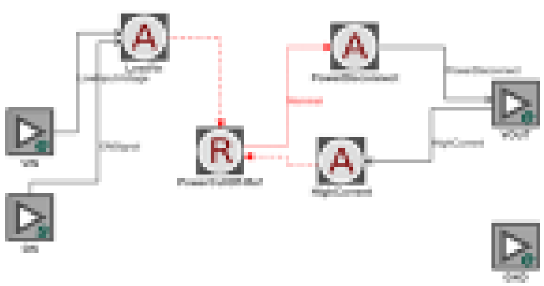


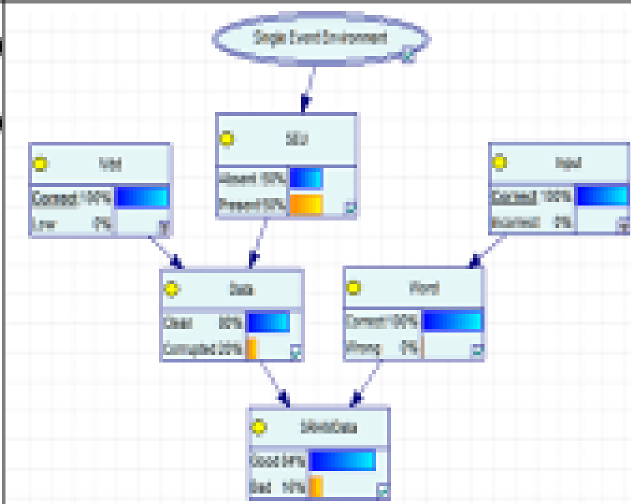
Overview of Modeling Languages Used - Model Based Systems Engineering (MBSE)

Overview of Modeling Languages Used

Vanderbilt Engineering

SysML	GSN	Bayes Net
• Specification of systems through standard notation • Added fault propagation paths	• Visual representation of argument • Goals, Strategies, and Solutions	• Nodes describe probabilities of states • Calculate conditional probabilities from observations





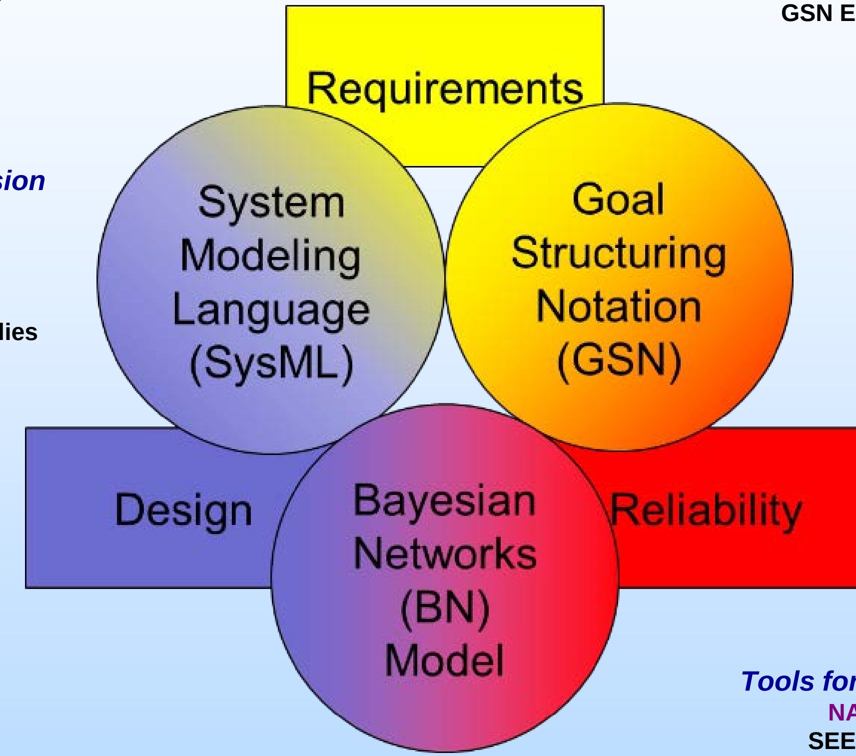
Presented at NASA Electronic Parts and Packaging (NEPP) Technical Interchange Meeting (TIM), Vanderbilt University, Nashville, TN, August 29-30, 2017.

NEPP (w/ NASA MBMA Program)
Pieces to the puzzle (partial)

Emerging Architecture
Vanderbilt University
Web-based tool (SEAM)

Developing Requirements and Goals
NASA/GSFC (Campola) - Vanderbilt
Notional RHA Tool (R-GENTIC)
NASA/GSFC (Xapsos)
RHA Confidence Approach

Exemplars and Training for MBMA
Vanderbilt University
GSN Exemplar (SEE) – complete
TBD
GSN Exemplar – EEE parts reliability



COTS Data
GSFC
NEPP/Radhome data
(+ collaborations)
GSFC
IEEE REDW access
GSFC/JPL (new data)
CubeSat EEE Parts Testing

Understanding the Small Mission Universe
Saint Louis University
CubeSat Success Study
JPL
CubeSat EEE Parts Database Studies
Aerospace (proposed)
CubeSat Kit Vendor Survey

Best Practices (Process and Test)
NASA/GSFC (Campola)
Small Mission RHA
NASA/GSFC
Small Mission EEE Parts Best Practices
NASA/GSFC (Xapsos)
RHA Confidence Approach
GSFC
Board Level Testing and EEE Part Reliability
JPL
Board Level Proton Testing

Knowledge Sharing
Integration with S3VI
(NASA/ARC)
GSFC
ESA Small Mission RHA

Tools for Radiation Reliability
NASA/GSFC (Berg)
SEE Classic Reliability
Vanderbilt
CRÈME Toolsuite
Vanderbilt
BN Model + Integrating into SEAM
NASA/GSFC (Xapsos)
RHA Confidence Approach

Reliable less than MIL
Aerospace (proposed)
Space Enhanced Performance
(SEP) Electronics Grade Study

TBD
Resilience, autonomy

https://modelbasedassurance.org/

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"!**

Five stages of Consumer Behavior

P. Kotler and G. Armstrong, "Consider Purchase Decision Process Model Reference," Principles of Marketing, 2001.