NASA and COTS Electronics: Past Approach and Successes – Future Considerations

Kenneth A. LaBel,

NASA Electronic Parts and Packaging (NEPP) Co-Manager

ken.label@nasa.gov

301-286-9936

Open Access

Acronym List

- **Bayesian Networks (Bayes Net)**
- **Bayesian Networks (BN)**
- **Command and Data Handling (CADH)**
- **Consultative Committee for Space Data Systems (CCSDS)**
- **Chemistry of Failure (COF)**
- **Commercial Off The Shelf (COTS)**
- **Displacement Damage Dose (DDD)**
- **Dead On Arrival (DOA)**
- **U.S. Department of Defense (DoD)**
- **Dynamic Random Access Memory (DRAM)**
- **Error Detection and Correction (EDAC)**
- **Electrical, Electronic and Electromechanical (EEE)**
- **Electrostatic Discharge (ESD)**
- **Geosynchronous Equatorial Orbit (GEO)**
- **Goddard Space Flight Center (GSFC)**
- **Goal Structured Notation (GSN)**
- **International Space Station (ISS)**
- **NASA Jet Propulsion Laboratory (JPL)**
- **Low Earth Orbit (LEO)**
- **Model-Based Mission Assurance (MBMA)**

- **Military/Aerospace (Mil/Aero)**
- **NASA Electronic Parts and Packaging (NEPP) Program**
- **Personal Computer (PC)**
- **Printed Circuit Boards (PCBs)**
- **Physics of Failure (PoF)**
- **real-time operating system (RTOS)**
- **Solar Anomalous Magnetospheric Particle Explorer (SAMPEX)**
- **Small Explorer Data System (SEDS)**
- **Single Event Effects (SEE)**
- **Single Event Upset (SEU)**
- **Small Explorer (SMEX)**
- **Surface Mount Technology (SMT)**
- **Static Random Access Memory (SRAM)**
- **Solid State Recorders (SSRs)**
- **Size, Weight, and Power (SwaP)**
- **Systems Modeling Language (SysML)**
- **Total Ionizing Dose (TID)**
- **Ultraviolet (UV)**
- **Virtual Real-Time Executive (VRTX)**

Abstract/Outline

- **NASA has a long history of using commercial grade electronics in space. In this talk, a brief history of NASA's trends and approaches to commercial grade electronics focusing on processing and memory systems will be presented.**

- **This will include providing summary information on the space hazards to electronics as well as NASA mission trade space.**

- **We will also discuss developing recommendations for risk management approaches to Electrical, Electronic and Electromechanical (EEE) parts and reliability in space.**

- **The final portion of the talk will discuss emerging aerospace trends and the future for Commercial Off The Shelf (COTS) usage.**

Sample Space Hazards by Orbit Type

	Plasma (charging)	Trapped Protons	Trapped Electrons	Solar Particles	Cosmic Rays	Human Presence	Long Lifetime (>10 years)	Nuclear Exposure	Repeated Launch	Extreme Temperature	Planetary Contaminates (Dust, etc)
GEO	Yes	No	Severe	Yes	Yes	No	Yes	No	No	No	No
LEO (low-incl)	No	Yes	Moderate	No	No	No	Not usual	No	No	No	No
LEO Polar	No	Yes	Moderate	Yes	Yes	No	Not usual	No	No	No	No
Shuttle	No	Yes	Moderate	No	No	Yes	Yes	No	Yes	Rocket Motors	No
ISS	No	Yes	Moderate	Yes - partial	Minimal	Yes	Yes	No	No	No	No
Interplanetary	During phasing orbits; Possible Other Planet	During phasing orbits; Possible Other Planet	During phasing orbits; Possible Other Planet	Yes	Yes	No	Yes	Maybe	No	Yes	Maybe
Exploration - Vehicles	Phasing orbits	During phasing orbits	During phasing orbits	Yes	Yes	Yes	Yes	No	Yes	Rocket Motors	No
Exploration – Lunar, Mars	Phasing orbits	During phasing orbits	During phasing orbits	Yes	Yes	Yes	Yes	Maybe	No	Yes	Yes

Note that this is not a complete space hazard list.

Other items such as operation in a vacuum, UV exposure, etc… aren't included.

The Space Radiation Environment

- **Three portions of the natural space environment contribute to the radiation hazard**
  - **Free-space particles**
    - **Galactic Cosmic Rays (GCRs)**
  - **Solar particles**
    - ***Protons* and heavier ions**
  - **Trapped particles (in magnetic fields)**
    - ***Protons* and electrons including the earth's South Atlantic Anomaly (SAA)**
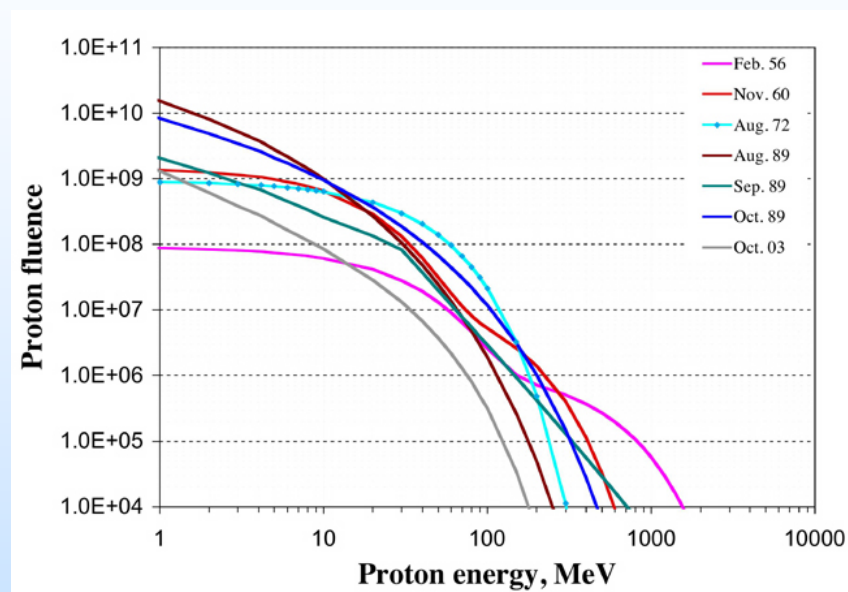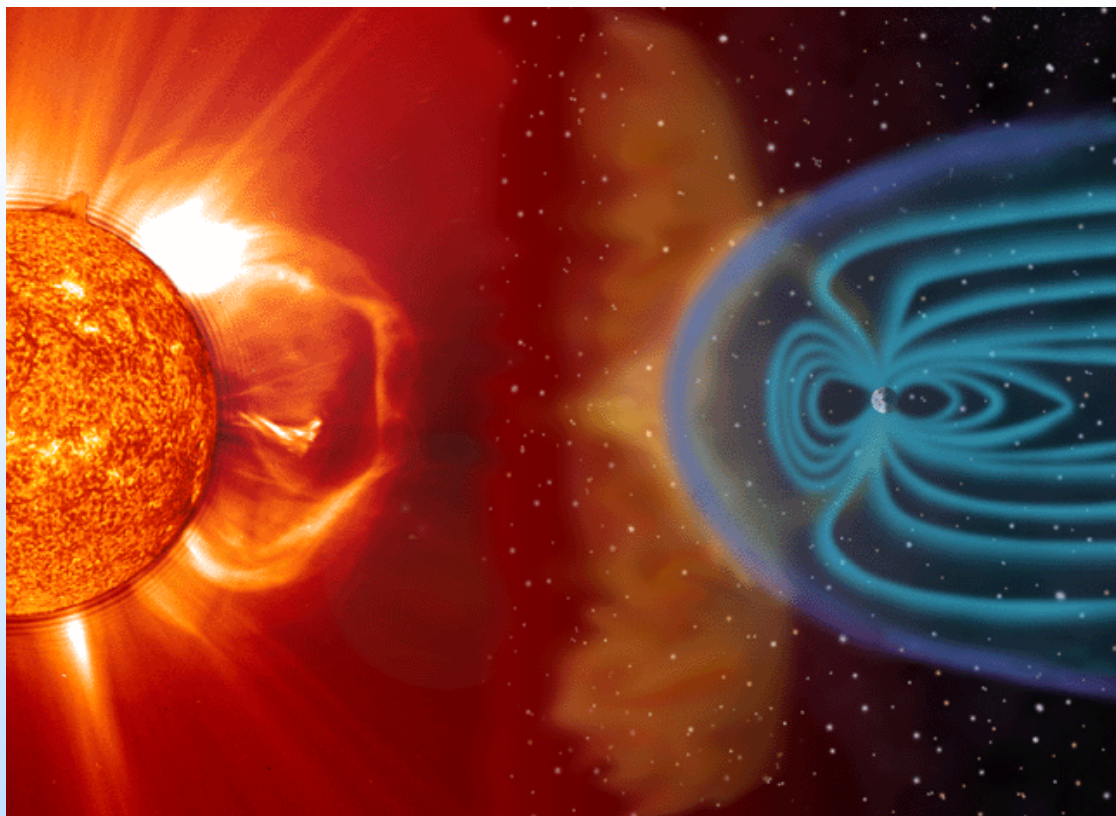- **Hazard experienced is a function of orbit and timeframe**

Image from the OLTARIS Web site [Singleterry et al., 2010] maintained by the NASA Langley Research Center

The Sun-Earth Radiation Environment

Sun (left) acts as a source of protons (solar events) and its solar cycle (max, min) modulates the environment

**Particles are trapped in the earth's magnetic fields (right)**

after K. Endo, Nikkei Sciences

Space Radiation Effects on Electronics

- **Long-term cumulative degradation**
  - **Ionization damage aka Total Ionizing Dose (TID)**
  - **Non-Ionizing Damage aka Displacement Damage Dose (DDD)**
- **Single particle effects (aka Single Event Effects or SEE)**
  - **Soft or hard errors caused by protons (mostly nuclear interactions) or heavy ions (direct energy deposition)**

Particle interactions with semiconductors

Image from the Space Telescope Science Institute (STScI), operated for NASA by the Association of Universities for Research in Astronomy

http://www.stsci.edu/hst/nicmos/performance/anomalies/bigcr.html

Atomic Interactions
  - **Direct Ionization**
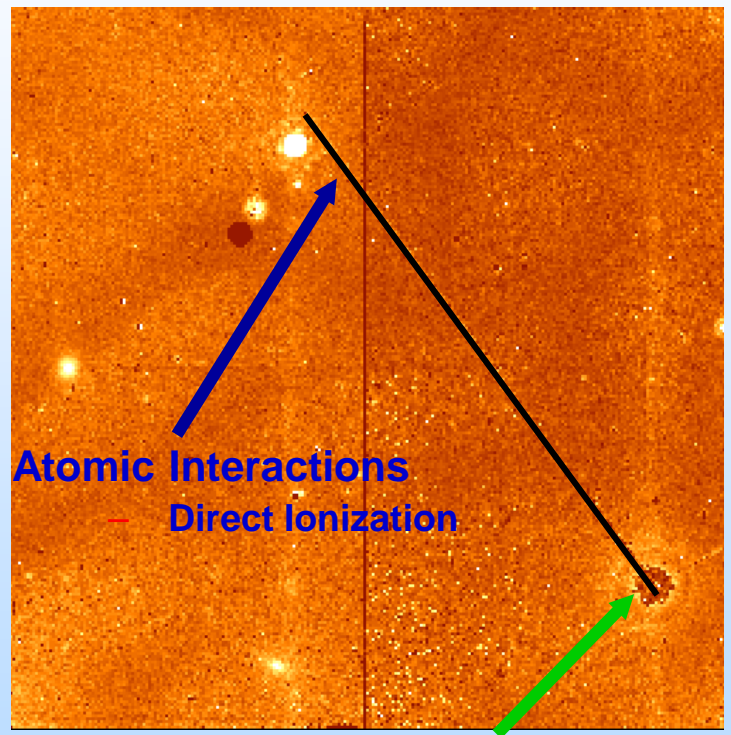
Interaction with Nucleus
  - **Indirect Ionization**
  - **Nucleus is Displaced**
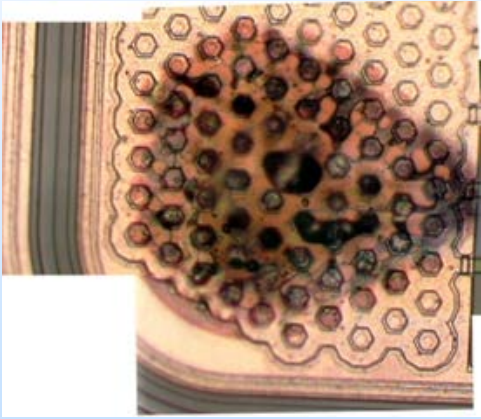 - **Secondaries spallated**

SEE Effects – Hard Failures During Particle Irradiation Testing
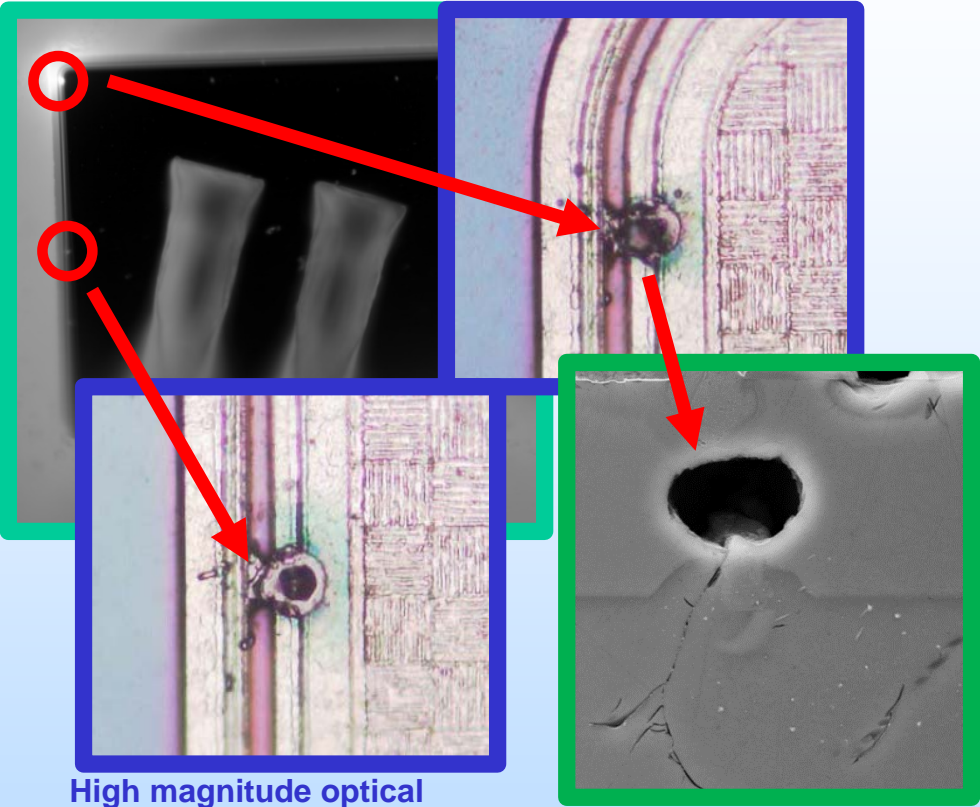
High magnitude optical images of failure locations

Cross-section of failure location

Failure images in a diode

Failure in a Power Device

These types of failures are MISSION ending!

Actual Space Anomalies Observed During Major Solar Event in 2003

Type of Event	Notes
Spontaneous Processor Resets in main computers	3 events; all recoverable
Spontaneous Processor Resets in main computers	Seen on other spacecraft; recoverable
Spontaneous Processor Resets in main computers	Spacecraft tumbled and required ground command to correct
High Bit Error Rates	Communication link
Magnetic Torquers Disabled	Guidance system
Star Tracker Errors	Excessive event counts in guidance system
Star Tracker Errors	Star Tracker Reset occurred
Read Errors	Entered safe mode; recovered
Failure	One mission failure noted
Memory Errors	19 errors on 10/29
Memory Errors	Increase in correctable error rates on solid-state recorders noted in many spacecraft

To be presented by Kenneth A. LaBel at SELSE 2018 14th IEEE Workshop on Silicon Errors in Logic System Effects, Boston, MA, April 3-4, 2018.

9

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…

Application/ Environment

Physics of failure (POF)

Chemistry of failure (COF)

Screening/ Qualification Methods

Mission Reliability/ Success
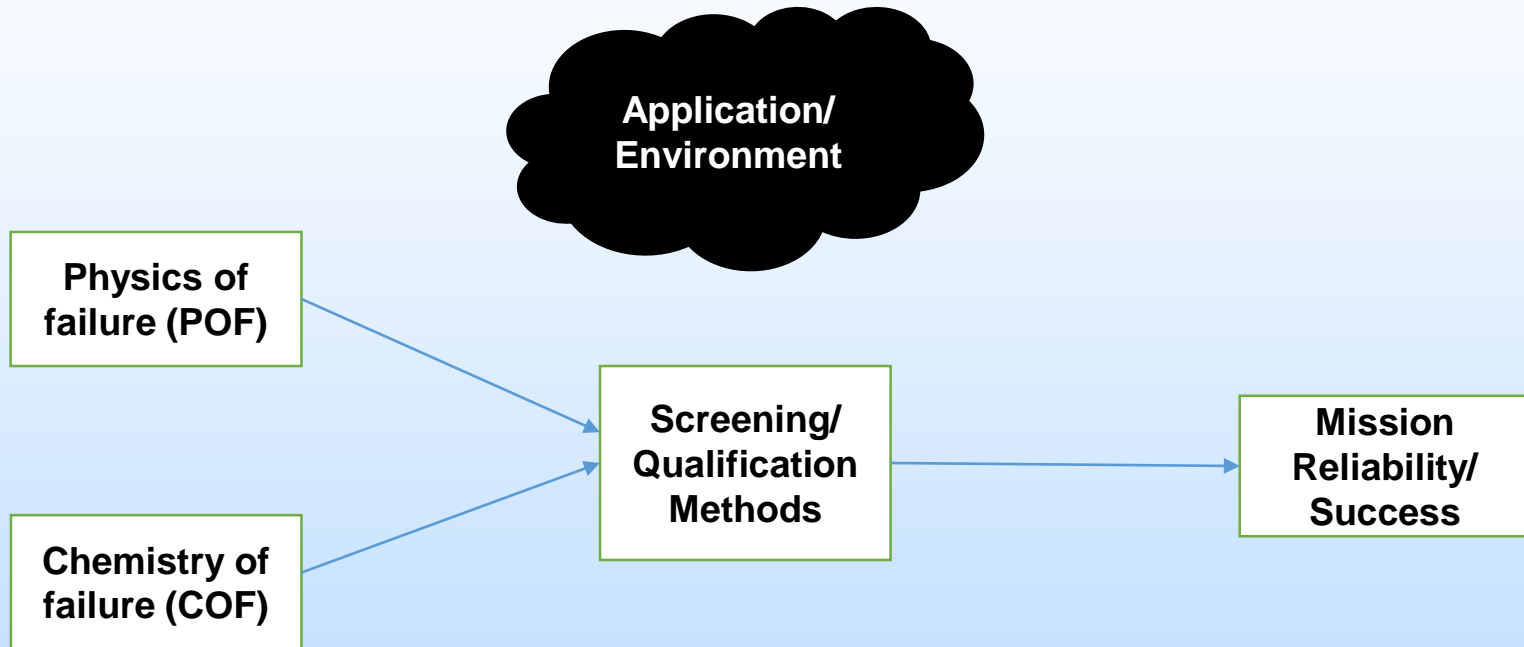
It's not only about the technology,

but perspective on safe usage in space programs.

RISK MANAGEMENT!
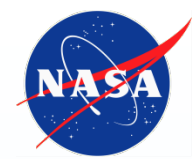
Reliability and Availability

- **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 work"
    - Less confidence in both reliability and availability.
   - It may work, but prior to flight there is less certainty.

CONFIDENCE LEVEL

- INDESTRUCTIBLE
- STURDY
- STABLE
- INCREASING
- FINE
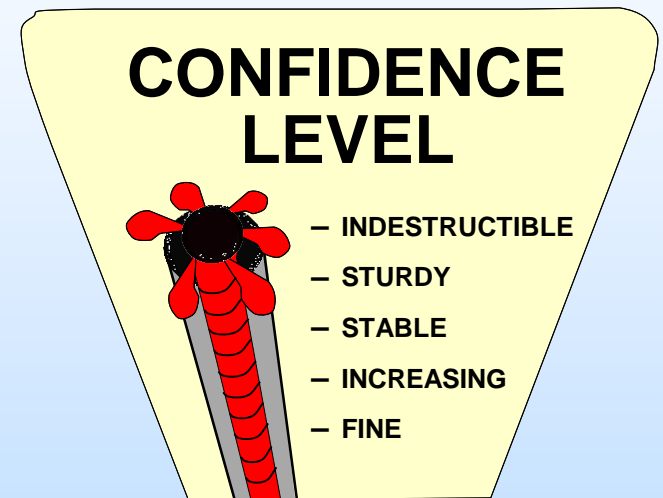
Traditional EEE Parts Approach to *Confidence*

- ## 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)
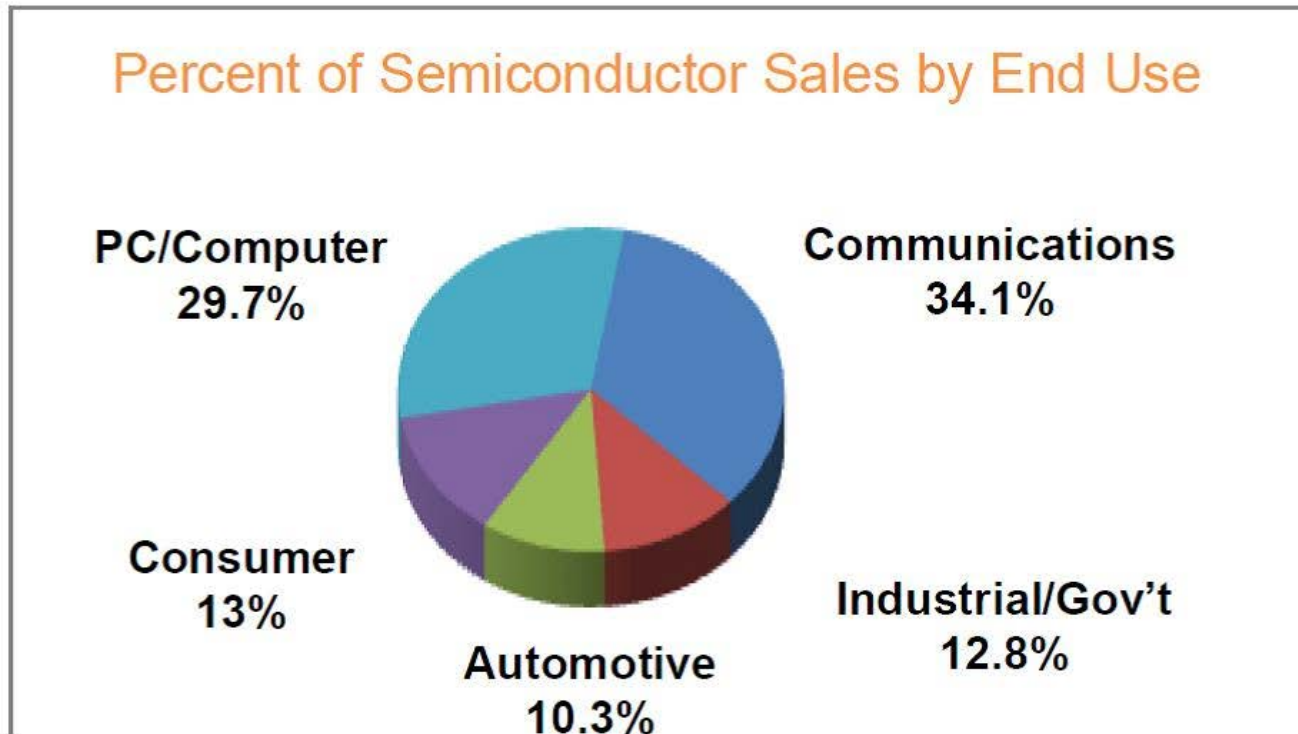   - *high confidence*
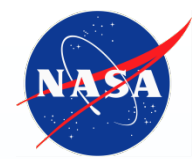
EEE parts are available in "grades"

- **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).**

A History Lesson

2015 Global Semiconductor Market: $335 Billion

Percent of Semiconductor Sales by End Use

PC/Computer 29.7%

Communications 34.1%

Consumer 13%

Automotive 10.3%

Industrial/Gov't 12.8%

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 (<1%)

Aerospace is a small percentage of this amount (<0.1%)

For comparison, in 1975, the Military and Aerospace market share was ~$50%!

Why NASA Has Used the Mil/Aero Grade

- **Prime reason has been the detailed and relevant knowledge about the performance and reliability of the actual parts to be flown.**

- **Mil/Aero uses a standardized set of manufacturer qualification tests that provide confidence in a device's reliability for a wide range of space conditions.**

  – **The test levels are set such that they bound the majority of environment and lifetime exposures for space missions with the exception of extreme environments and, in some cases, radiation tolerance.**

  – **Mil/Aero also allows manufacturers to perform one set of qualification tests rather than a tailored set for each specific mission environment and lifetime profile.**

Risk Avoidance Approach

NASA COTS Challenges

- **Unique Space Usage Constraints**
  - **Environment hazards**
  - **Servicing (limited options)**
  - **Wide range of mission lifetimes and orbits**
  - **System availability (not just reliability) requirements (criticality of function and timing)**

Solution Details

Quality / Reliability / Cost →

	COTS	Q100	EP	QMLQ	Space EP*	Space-QMLV
Packaging	Plastic	Plastic	Plastic	Ceramic	Plastic	Ceramic
Single Controlled Baseline	No	No	Yes	Yes	Yes	Yes
Bond Wires	Au/Cu	Au/Cu	Au	Al	Au	Al
Is Pure Sn used?	Yes	Yes	No	No	No	No
Guaranteed Rad Performance	No	No	No	No	Yes	Yes
Typical Temp Range	-40°C - 85°C	-40°C - 125°C	-55°C - 125°C (majority)	-55°C - 125°C	-55°C - 125°C	-55°C - 125°C
Extra Qual and Process Monitors	No	Yes	Yes	Yes	Yes	Yes
Life Test Per Wafer Lot	No	No	No	No	Yes	Yes
Orderable by Single Lot	No	No	No	Yes	TBD	Yes

*Space EP currently in definition

Used by permission from the author, Robert Baumann, "From COTS to Space - Grade Electronics: Improving Reliability for Harsh Environments," 2016 Single Event Effects (SEE) Symposium and the Military and Aerospace Programmable Logic Devices (MAPLD) Workshop, La Jolla, CA, May 23-26, 2016.

For a small market (compared to commercial),

space electronics place big demands on the semiconductor manufacturer.
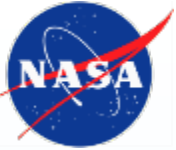
The Move to COTS in Space

- **Up until 1990 timeframe, NASA used COTS mainly in cases where no Mil/Aero alternative existed or in some non-critical applications.**

- **However, key performance parameters (size, weight, and power – SwaP as well as processing system performance) began to drive the usage of COTS into mainstream applications within the Agency.**

  - **Example: the evolution of space data recorders**
    - **1960's-70's - Magnetic Core Memory**
    - **1970's-80's - Magnetic Tape Recorder**
    - **1990's - Solid State Recorders (SSRs) – Static Random Access Memory (SRAM)**
    - **Late 1990's - SSR – Dynamic Random Access Memory (DRAM)**
    - **Early 2010's - SSR – FLASH**

Apollo Guidance Computer
- **4 kB of Magnetic Core Memory**
  Courtesy NASA Archives

NASA's Approach to Using COTS Electronics – The "Old" Way

- **The classic approach is called *upscreening*:**
  - Perform a series of tests over extended environment/lifetime parameters coupled with application usage information to determine if a part can meet a mission's reliability/availability constraints.
  - This includes temperature, vacuum, radiation, shock, vibration, etc…

- **While the confidence in the reliability/availability of this approach may be less than electronics designed for the harsh space environment, sufficient risk reduction may be achieved.**
  - Starting around 1990, NASA missions that had multi-year operation or significant radiation requirements began coupling COTS parts into systems usually with a salient mix of Mil/Aero parts and fault tolerant architectures.

Example:
Solar Anomalous Magnetospheric Particle Explorer (SAMPEX)

- **On November 13, 2012, the SAMPEX spacecraft reentered the earth's atmosphere.***

- **SAMPEX, the first of NASA's Small Explorer (SMEX) spacecraft, was launched in 1992 with a three year design *lifetime* (5 year goal).**

- **It lasted operationally nearly twenty years due to a myriad of testing, electronic parts selection, and system architecture, thrilling the scientific investigators who were able to obtain tremendous new scientific data.**

- **One should note that the entire spacecraft was designed, built, and validated in three years (1989-1992) by NASA.**

  - **Its orbit was a slightly eccentric low earth polar orbit.**

https://www.nasa.gov/images/content/700355main_ sampex_full.jpg

* = Karen C. Fox, "NASA's SAMPEX Mission: A Space Weather Warrior," NASA/GSFC, Nov. 01,2012, http://www.nasa.gov/mission_pages/sunearth/news/sampex-deorbit.html

SAMPEX's Command and Data Handling (CADH) System -
The Small Explorer Data System (SEDS)

- **SEDS was built upon traditionally competing ideas:**
  - Increasing spacecraft performance, and,
  - Having a high reliability/availability spacecraft.
- **This led, in itself, to two concepts for the CADH:**
  - Selection of commercial and new electronics technologies, and,
  - Detailed evaluation (technology), qualification, and validation planning.
- **The SEDS approach became the cornerstone philosophy and system design for generations of spacecraft that followed.**

The SEDS Architecture

after D. N. Baker, et al, "The Solar, Anomalous, and Magnetospheric Particle Explorer (SAMPEX) Mission," IEEE Transactions on Geoscience and Remote Sensing, Vol. 31, No. 3, May 1993, pp. 531-541

SEDS Technology: Fiber Optics

- **Development and first use of a fiber optic data bus (MIL-STD-1773).**
  - This included selection and testing of the optical and electrical components, protocol electronics, connectors, couplers, and optical fiber.
  - Radiation testing was partnered with U.S. Department of Defense (DoD) (Naval Research Labs) which has led to continued collaboration between our organizations.

- **MIL-STD-1773 was also the first NASA move away from traditional custom parallel bus structures for data/command transfer to serial bus structure.**
  - This simplified interconnects and was a size, weight, and power (SWAP) savings breakthrough.
  - The underlying electrical protocol, MIL-STD-1553, is still in common use across the space industry and paved the way for newer generations of databus implementations such as SpaceWire.
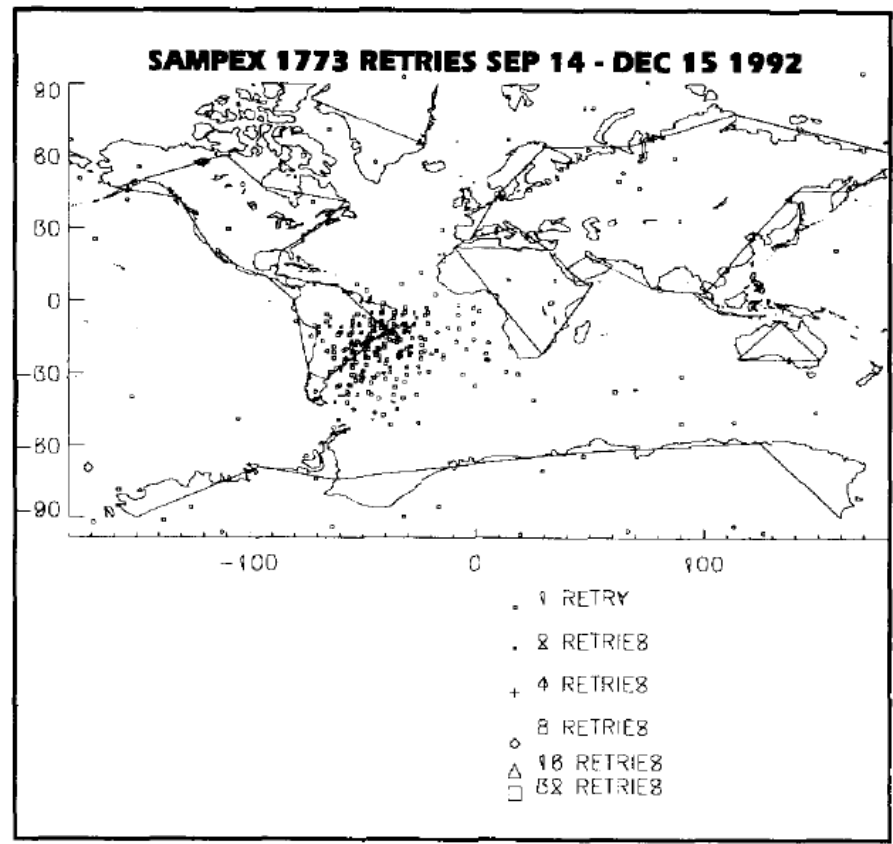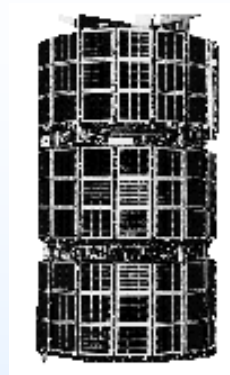

SAMPEX 1773 RETRIES SEP 14 - DEC 15 1992

- 1 RETRY
- 2 RETRIES
+ 4 RETRIES
◇ 8 RETRIES
△ 16 RETRIES
□ 32 RETRIES

Figure 11   SAMPEX 1773 retries over Mercator projection

after K.A. LaBel, et al, "SEDS MIL-STD-1773 Fiber Optic Data Bus: Proton Irradiation Test Results and Spaceflight SEU Data," IEEE Transactions on Nuclear Science, Vol. 40, No. 6, Dec 1993
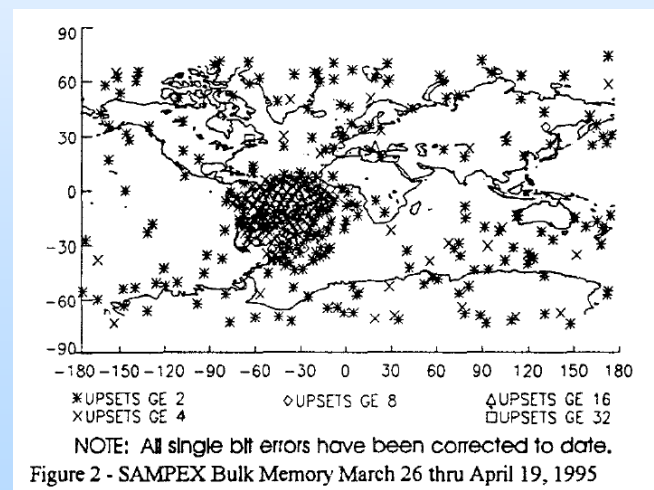
SEDS Technology: SSR

- **First NASA use of COTS SRAM as means of building a SSR.**
  - A Hitachi 32k x8 SRAM device was used and tested by the Aerospace Corporation for radiation tolerance prior to insertion.
  - The Air Force (P87-2 Mission) had flown this SSR design as an experiment previously.
  - In addition, fault tolerance (Hamming Code Error Detection and Correction (EDAC)) was included to deal with the expected single event upset (SEU) radiation hits.

- **The SSR was also the first use of surface mount technology (SMT) in a NASA spacecraft.**
  - SMT replaced through-hole mounting of devices to printed circuit boards (PCBs), thus allowing for two-sided PCB usage and more compact (physical) designs.
  - A detailed series of thermal vacuum and shock/vibration testing was performed on test coupons to determine "safe usage" and rules were developed for the SAMPEX products and subsequently used by other NASA missions.

P87-2 circa 1990
1st known spaceflight SSR
Air Force release pic from the P87-2 mission (aka Stacksat)
http://www.thespacereview.com/article/2104/1

NOTE: All single bit errors have been corrected to date.
Figure 2 - SAMPEX Bulk Memory March 26 thru April 19, 1995

after C.M. Seidleck, et al, "Single Event Effect Flight Data Analysis of Multiple NASA Spacecraft and Experiments; Implications to Spacecraft Electrical Designs," IEEE Proceedings of the Third European Conference on Radiation and its Effects on Components and Systems, 18-22 Sept. 1995

SEDS Technology:
COTS 32-bit Processor (1)

- **The first use of a commercial 32-bit processor in a NASA spacecraft**
  - **INTEL 80386 and its peripheral support ICs.**
- **This drove development of a number of new features for space electronics:**
  - **Extensive radiation test campaign by GSFC and JPL on the 80386 processor family at the part level. This drove initial designs for fault tolerance.**
  - **A seven layer fault tolerant system that included:**
    - **a watchdog processor,**
    - **software task monitors,**
    - **multi-day timeout, and more.**
    - **Key Feature: the fault tolerance was based on dissimilar strings.**
      - **A radiation hardened 80C86RH processor was used as a watchdog for the main processor**

SEDS Technology:
COTS 32-bit Processor (2)

- **This drove a number of new features into and of itself (cont'd):**
  - *A full system validation test under radiation exposure* **(i.e., an engineering model was taken to a heavy ion test facility along with the full ground system).**
    - **Various chips were exposed sequentially.**
    - **Upsets/anomalies were noted and the system would utilize its fault tolerant features to recover.**
    - **A small number of unrecoverable events were noted and system workarounds were then designed in. This was teamwork at its best.**
  - **First use of a commercial real-time operating system (RTOS): Ready Systems' Virtual Real-Time Executive (VRTX) and the "C" programming language.**
  - **Development and use of a deterministic software bus concept.**
 - **First true implementation of the Consultative Committee for Space Data Systems (CCSDS) "Blue Book" by NASA.**

Changing Dynamics for Space

- **Cost constraints and cost "effectiveness" have led to dramatic shifts away from traditional large-scale missions (ex., Hubble Space Telescope) that utilize traditional assurance approaches.**

- **Two major trends in the aerospace community are driving the use of more non-space/radiation hardened products:**
  - **The advent of small spacecraft such as CubeSats**
    - **A different risk acceptance profile versus mission purpose and cost**
  - **The increased use of "commercial" space providers**
    - **The procuring agent "buys" a service or data product and the implementer is responsible for ensuring mission success with limited agency oversight**
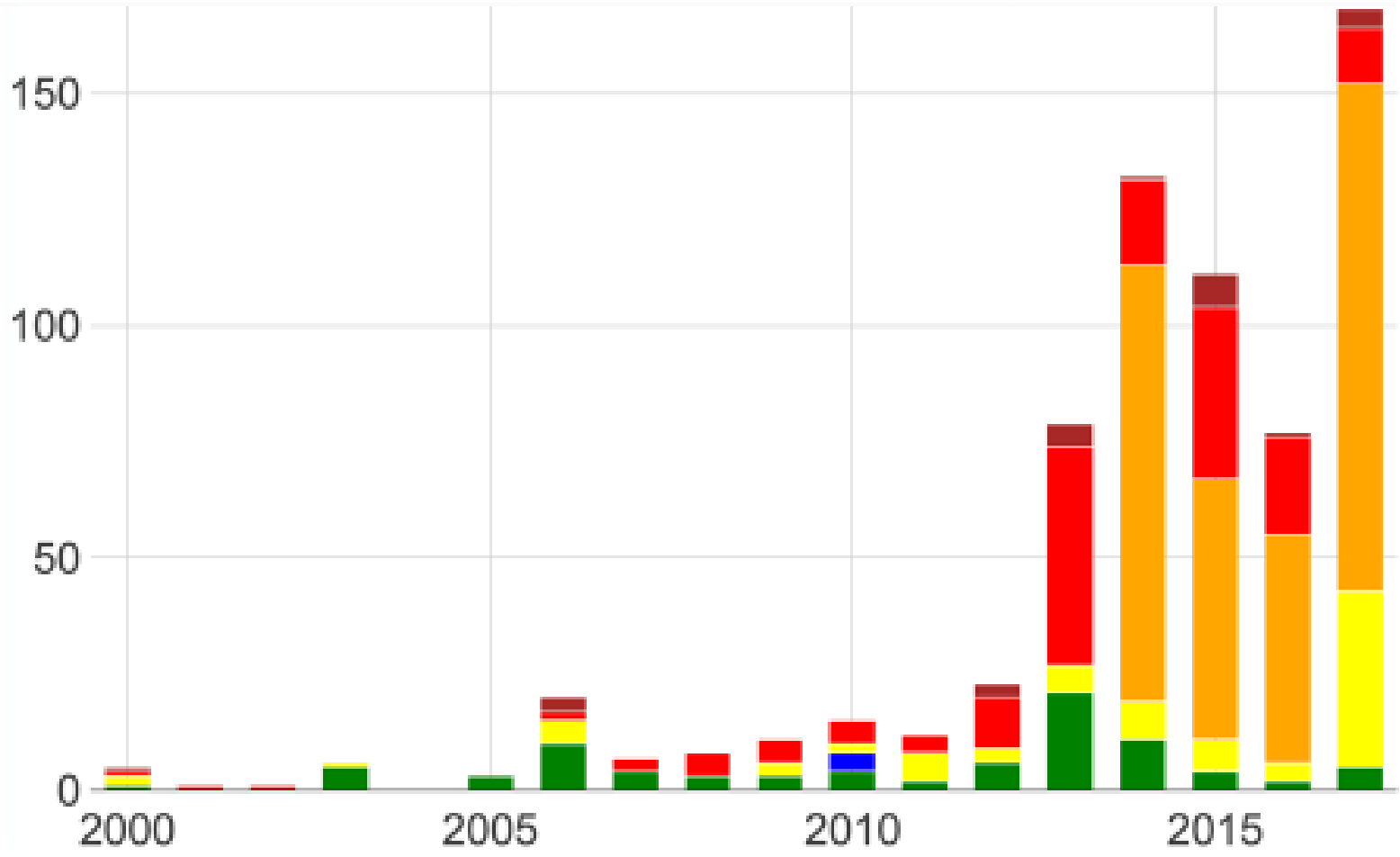
CubeSats Launched (2000-2017)
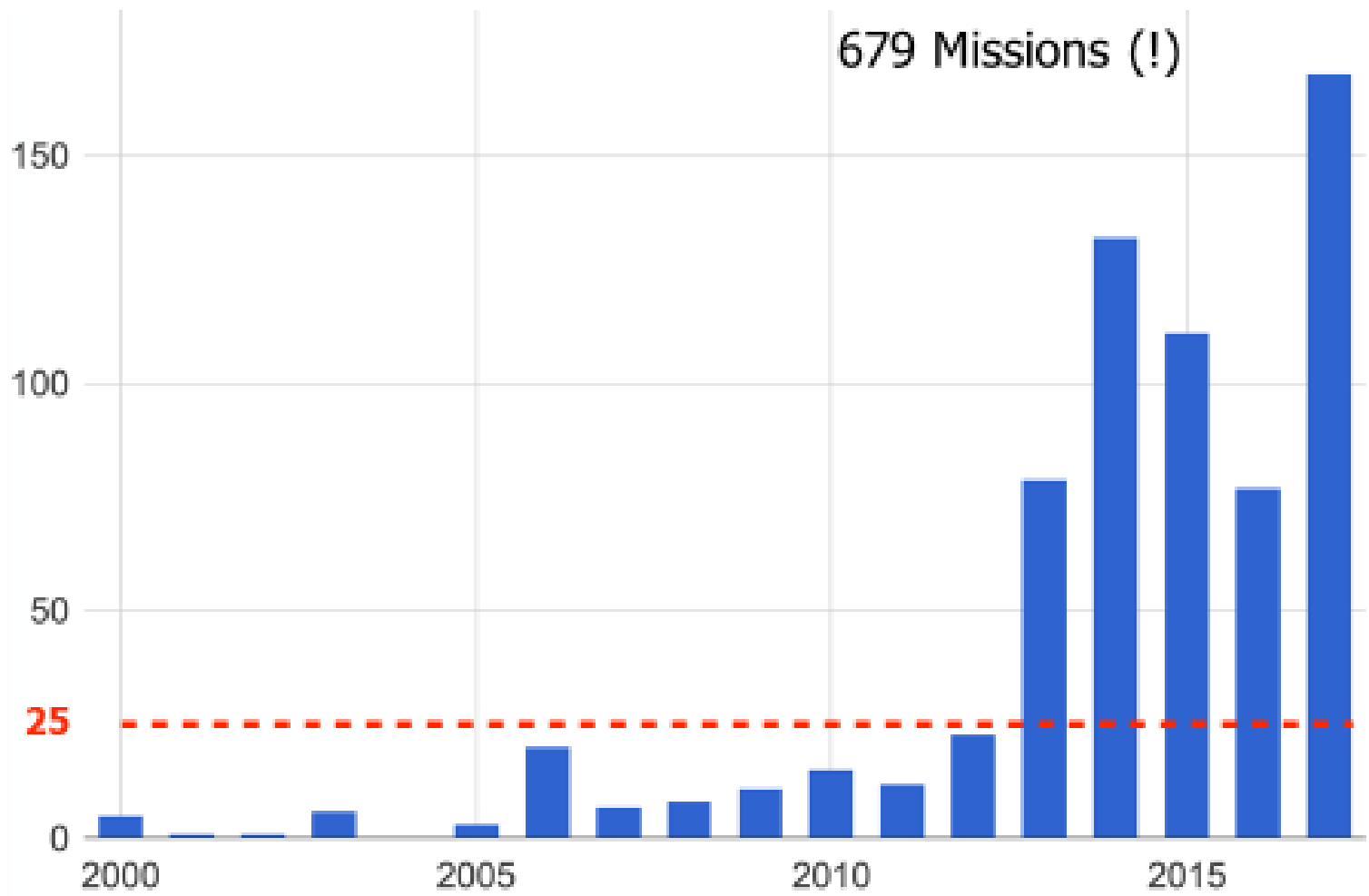
679 Missions (!)

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
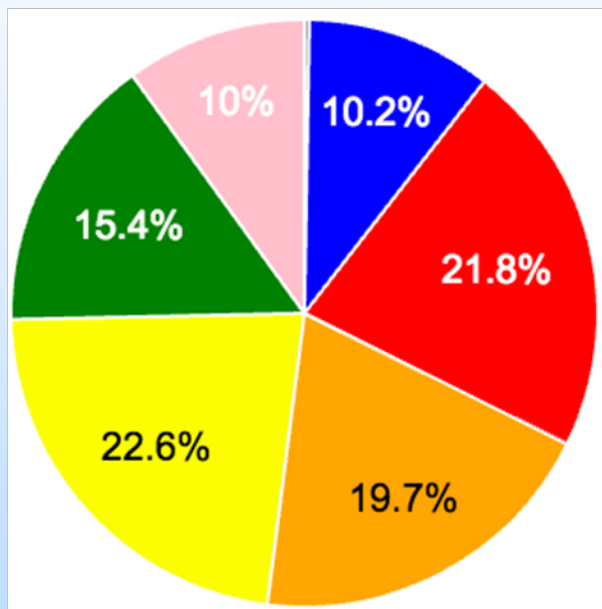

Michael Swartwout, "CubeSat Mission Success: 2017 Update (with a closer look at the effect of process management on outcome),"
NASA Electronic Parts and Packaging (NEPP) Program, 2017 NEPP Electronics Technology Workshop, June 26-29, 2017.
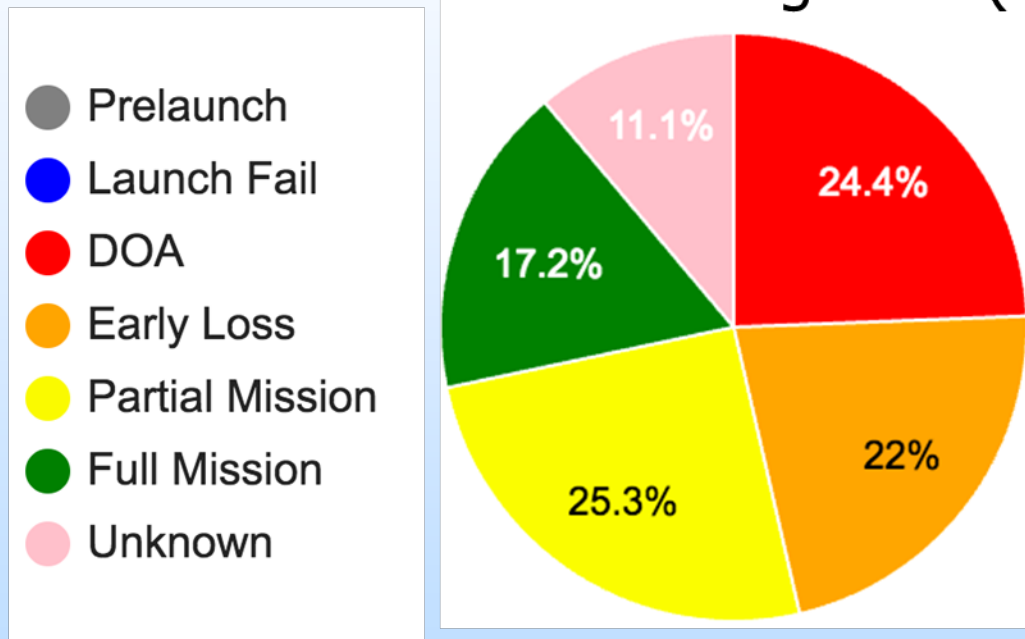
CubeSat Success?

All Missions (371)

Launch Fail: 10.2%
DOA: 21.8%
Early Loss: 19.7%
Partial Mission: 22.6%
Full Mission: 15.4%
Unknown: 10%

Legend:
- Prelaunch (gray)
- Launch Fail (blue)
- DOA (red)
- Early Loss (orange)
- Partial Mission (yellow)
- Full Mission (green)
- Unknown (pink)

All missions reaching orbit (332)

DOA: 24.4%
Early Loss: 22%
Partial Mission: 25.3%
Full Mission: 17.2%
Unknown: 11.1%

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.
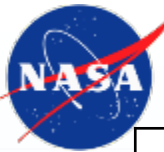
NASA's Changing Landscape

- **With NASA's new era of commercial providers and small space missions (i.e. CubeSats, etc…) other approaches are being considered to find more cost-effective approaches to meeting mission requirements.**
  - **These trends are driving the usage of non Mil/Aero parts such as Automotive grade.**

- **A few of the considerations for this emerging space include, but are not limited to:**
  - **Increased reliance on fault tolerance, architectural reliability approaches, and even constellation spacecraft sparing,**
  - **Leverage on the improved defect reliability of high yield COTS, automotive, industrial, and medical grades of electronics,**
  - **Use of higher-assembly level testing,**
  - **Reliance on new tools for model-based mission assurance (MBMA), circuit simulation and verification, as well as physics of failure (PoF), and,**
  - **Improved communication on considerations, lessons learned and guidelines.**

The Modern Approach to EEE Parts

- **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 illustrates an 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	Low (Environment/Lifetime)	Medium (Environment/Lifetime)	High (Environment/Lifetime)
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.**

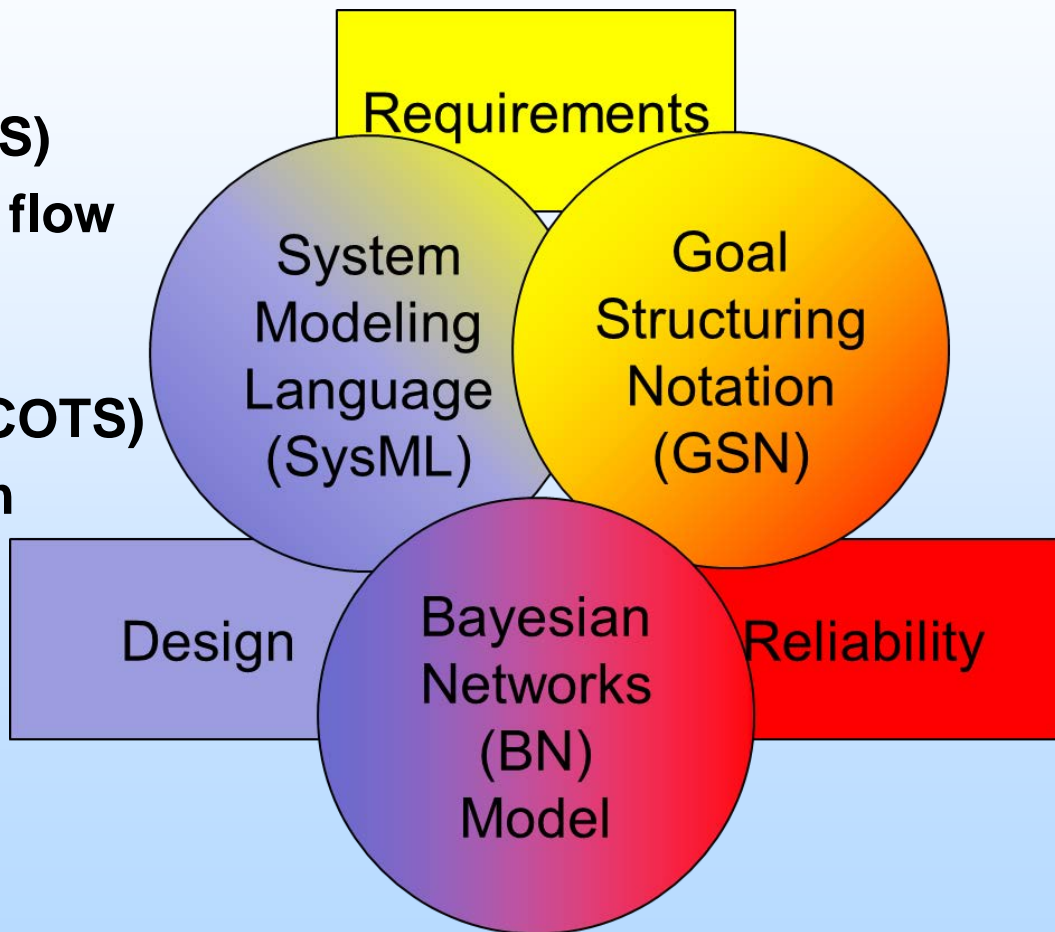- ***All fault tolerance must be validated.***

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

Model Based Mission Assurance (MBMA)-
A New Consideration for EEE Parts Assurance

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

Requirements

System Modeling Language (SysML)

Goal Structuring Notation (GSN)

Design

Bayesian Networks (BN) Model

Reliability

https://modelbasedassurance.org/

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

10

To be presented by Kenneth A. LaBel at SELSE 2018 14th IEEE Workshop on Silicon Errors in Logic System Effects, Boston, MA, April 3-4, 2018.

37

Lessons Learned on COTS for Space (1)

- **In an ideal world (and given limitations of testability, time, and budget),**
  - **Test at the device level to provide input for fault tolerant design. And,**
  - **Test at the system level to validate design approaches**
    - **Possibly uncover additional fault modes (statistics of test coverage).**

Many entities are trying to do the 2nd and mistakenly calling it qualification when it's really a "system validation" (with some inherent risk)…

Lessons Learned on COTS for Space (2)

- **Methods for evaluating risk in a more "system" manner are increasing based on risk profiles and architectures**
  - **MBMA is one possible means for streamlining**
- **Understanding the criticality of the application is the key to performing adequate testing and validation for risk management**
  - **However, even "good" ground testing and designs can be surprised (anomalies/failures)**
    - **Example: The random/Markov nature of SEEs and challenges related to "completeness" of sufficient testing (time, resources)**

Summary

- **An overview of NASA's changing considerations for EEE Parts Assurance was presented**
- **This has included**
  - **Background material on the challenge for COTS in space and traditional methodologies,**
  - **Examples from the SAMPEX mission of COTS/new technology insertion,**
  - **The changing space business,**
  - **A discussion of a recommended assurance approach and new methods, and,**
  - **A few lessons learned as takeaways.**