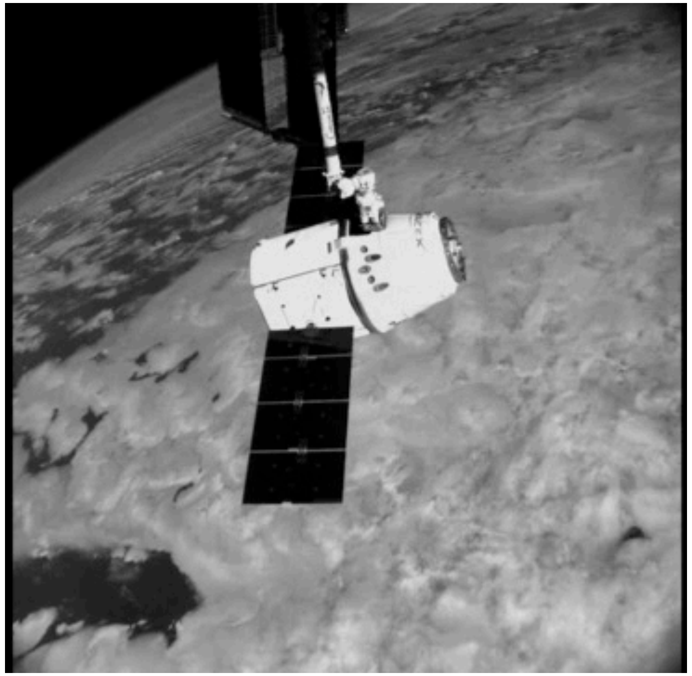
Approaches for Phasing Commercial-Off-The-Shelf Electronic Parts into NASA Missions

Key NESC Phase I study results and NASA GSFC recommendations*



(Phase I Report)

NESC-TI-19-01490

Jesse Leitner, Code 300
Dave Petrick, Code 560
Chris Green, Code 560
Robert Hodson, NESC Lead
Yuan Chen, Technical Lead

Hearts, minds, and culture*

- When mission success has prevailed and processes have remained the same for decades, it is hard for people to conceive that change is in order
  - Not everyone understands that in almost every significant field continuous improvement and the perpetual need to do more with less are essential
  - In some cases we don't recognize or appreciate the changing world around us or that we may be in process of being surpassed.
- Change has been a long haul, especially for Class B national asset missions because for practices that have long been perceived as critical for mission success, a "money is no object" approach has been taken with the perception that the risk and financial impacts of those processes are as simple as "essential to reliability" and "a small percentage of the budget"
  - In some cases, no amount of data, analysis, and overall evidence are sufficient to change the culture
  - Of course there is a comfort that if I do what we've always done and we fail, then I am covered, but if I am part of a change that is perceived as trying to save a few pennies, then I will be blamed
  - Some change will have to be forced through and stakeholders, customers, and developers must all contribute to the change.

Scope of the NESC Assessment

1. Discuss and summarize the various parts standards and approaches used by CCP partners, including parts selection, evaluation, screening, and qualification processes and criteria, and lessons learned from CCP parts leads/team and potentially from CCP partners.

2. Discuss, compile, and summarize the state of practices and/or best practices on use of COTS EEE parts for various programs/projects at NASA centers. The practices and best practices should provide the correlation between parts selection, evaluation, screening, and qualification process with respect to project category/classification, and address Mission, Environment, Applications and Lifetime (MEAL) for COTS EEE parts.

3. Based on 1) and 2), develop recommendations that could lead to future NEPP Program and/or agency guidance on COTS parts selection, evaluation, screening, qualification, and usage in space systems to perform as required over the life cycle for all types of space missions, by leveraging the lessons learned from CCP and the best practices currently being used across the agency.

Team List

Name	Discipline	Organization
Core Team		
Robert Hodson	NESC Lead, NASA Technical Fellow for Avionics	LaRC
Yuan Chen	Technical Lead, Parts Eng. and Reliability	LaRC
Carlton Faller	Parts Engineering	JSC
Ron Hodge	Parts/Packaging/FA	MSFC
Michael Defrancis	Parts/Packaging, SMA	JSC/SAIC
Kuok Ling	Parts Engineering	ARC
Chris Green	Parts Engineering	GSFC
Scott Gore	Parts Engineering	JPL
John Pandolf	Parts Engineering	LaRC
Erik Denson	Electrical Chief Engineer	KSC
Kristen Boomer	Parts Engineering	GRC
Angela Thoren	Parts Obsolescence	MSFC
Pete Majewicz	NEPP Manager	OSMA/GSFC
Michael Sampson	NEPAG Manager	OSMA/GSFC
Jesse Leitner	SMA	GSFC
Consultants		
Kathy Laird	Parts Engineering/FA	MSFC/NEPAG
Ray Ladbury	Parts Radiation	GSFC
David Petrick	SMA	GSFC
Jonathan Pellish	NASA EEE Parts Manager	GSFC
Dwayne Morgan	Avionics	WFF
Chris Iannello	NASA Technical Fellow for Electrical Power	KSC
Business Management		
Rebekah Hendricks	Program Analyst	LaRC/MTSO
Assessment Support		
Melinda Meredith	Project Coordinator	LaRC/AMA
Linda Burgess	Planning and Control Analyst	LaRC/AMA
Erin Moran	Technical Editor	LaRC/AMA

Participation from 8 centers:
ARC, GRC, GSFC, JPL, JSC, KSC, LaRC, MSFC

Engineering, SMA, NEPP, CCP

Agency Baseline Parts Requirements

- NASA-STD-8739.10 and GSFC EEE-INST-002 (Code 562 branch instruction) (and equivalent parts documents) establish the baseline requirements for use of various levels of parts including use of COTS parts.
  - NASA-STD-8739.10 establishes "a set of requirements at the Agency level to control risk and minimize the impacts of part selection and usage on reliability in NASA spaceflight hardware and critical GSE";
  - GSFC EEE-INST-002 (and equivalent parts documents) is used at Agency and Center levels for guidance on parts selection, screening and qualification requirements.
    - EEE-INST-002 is in the process of being revised to NASA-STD-8739.11
- Those documents recommend MIL-SPEC parts as the first choice or best practice, and specify
  - Different levels of MIL-SPEC parts as baseline parts, AND
  - Detailed MIL-SPEC/NASA screening and qualification requirements on non MIL-SPEC parts.
- <u>Most current practices use "NASA screened COTS", i.e., COTS qualified and screened using MIL standards per EEE-INST-002.</u>
- <u>Agency guidance in NASA-STD-8739.10 and in the new rev of NPR 8705.4 is to use Level 4 parts (commercial parts with no additional screening or qual) for Class D, which is not defined in EEE-INST-002</u>
  - <u>While GSFC practices in the past typically applied Class A or B practices for Class D projects, this was from a time when resources were not especially constrained and the impact of application of excessive practices to constrained projects was not well understood.</u>

MIL-SPEC parts vs. COTS parts

- **COTS Part:** A Commercial-Off-The-Shelf part designed for commercial applications for which the part manufacturer solely establishes and controls the specifications for performance, configuration and reliability, including design, materials, processes, and testing without additional requirements imposed by users and external organizations. It is typically available for sale through commercial distributors to the public with little or no lead time.
- Government control or insight
  - Government has control of and insight into MIL-SPEC parts, often resulting in parts with high (but not perfect) quality and reliability and full access to part-level verification.
  - Government does not have control or insight into COTS parts, resulting in a major challenge of part-level verification or guaranteed knowledge of COTS parts based on our current processes.
- Does it mean COTS parts are low in quality and reliability? Not necessarily.
  - Government control is not prerequisite anymore for high quality and reliability parts, especially when, in recent years, some manufacturers in commercial industry have developed rigorous process controls driven by advanced technologies and commercial market, often equivalent to or exceeding government controls on MIL-SPEC parts.
  - Equally important to note that this is not universally the case, and may vary from manufacturer to manufacturer.
- It should be noted that there was no evidence provided for reduced reliability with COTS parts on their own merits in the study compared to parts meeting Agency requirements

New Terminology Defined: Industry Leading Parts Manufacturers

- Defined an *Industry Leading Parts Manufacturer (ILPM)*
  - A parts manufacturer with high volume automatic production facilities that can provide documented proof of the technology, process and product qualification, and its implementation of the best practices for “zero defects” for parts quality, reliability and workmanship.
  - Detailed criteria of ILPM and part-level verification criteria to be addressed in Phase II.
- Recommended selecting COTS parts from *Industry Leading Parts Manufacturers*.
  - Take advantage of what commercial industry does the best – high volume automatic production manufacturer

Radiation Hardness Assurance on COTS parts

- Most MIL-SPEC parts and COTS parts are not designed for space applications.
- Even MIL-SPEC parts that are designed for atmospheric or terrestrial strategic applications may not perform adequately in space, because the space radiation environment is quantitatively and qualitatively more severe than that of the atmosphere.
- Radiation threats for COTS parts do not differ from MIL-SPEC parts
- Parts levels in EEE-INST-002 and equivalent documents do not indicate the level of radiation tolerance, and thus the selection of parts level 1, 2, or 3 does not imply or provide any type of radiation hardness or mitigation of radiation effects.
- The radiation hardness assurance guideline for COTS parts or any EEE part will be included in NESC-RP-19-01489 "Guidelines for an Avionics Radiation Hardness Assurance" (on-going assessment currently writing its final report).

Findings (I): COTS parts for spaceflight systems

- **F-1** For safety and mission critical systems on missions with Category 1-3, Class A-D, and sub-Class D, NASA has a long history of using NASA-screened COTS parts (i.e., by performing additional and full part-level screening and space qualification on the COTS parts per GSFC EEE-INST-002 or equivalent documents before incorporating them into the spaceflight system(s).
  - **F-1a.** For safety and mission critical systems on Category 1-3 and Class A-C missions, NASA Center current practices typically use NASA-screened COTS parts.
  - **F-1b.** For mission critical systems on Class D and sub-Class D missions, there is a wide range of differences in current Centers' practices on COTS selection and part-, board-, and system-level verification.
- F-2 For non-safety or non-mission critical systems, current center use of COTS practices range from using NASA-screened COTS parts to the best effort on part-level verification, or using COTS parts without any further MIL-SPEC/NASA screening and qualification at part-level, depending on mission classification level, project requirements and risk posture.
- F-3 NASA has more than 15 years of using COTS without additional part-level MIL-SPEC/NASA screening and qualification in space systems in sub-Class D missions and some Class D payloads, and other non-critical applications, some in complex systems operating for years. Most of those COTS parts were from Industry Leading Parts Manufacturers.
- F-4 There is a lack of consensus within NASA on the perception of risk of using COTS parts for safety and mission critical applications in spaceflight systems. It varies from feelings of "high risk" when part-level MIL-SPEC/NASA screening and space qualification are not fully performed to "no elevated risk" when sound engineering is used and part application is understood.
- F-5 Compared to MIL-SPEC parts, part-level verification for COTS parts used in spaceflight systems remains a major challenge, since there is no government insight or direct/formal communication channel existing with the COTS parts manufacturers.
- F-6 Not all COTS parts are created equal due to wide variability in parts manufacturers' process control and quality assurance.
- F-7 COTS parts, and most MIL-SPEC parts, are not designed and manufactured for space environments.

NESC Recommendations: COTS risk identification and mitigation

R-1. Programs/Projects should understand and effectively manage the risk of COTS, using a holistic approach incorporating inputs from across the project/program to make informed decisions and mitigate risk. ***(F-1, F-2, F-3, F-4, O-7)***

- Risk should be considered in the appropriate context, based on knowledge of the parts being used, the manufacturers, and how the parts are being used.

R-2. When COTS parts are used in safety or mission critical applications without any further part-level MIL-SPEC/NASA screening and space qualification, a mission specific COTS approach tailored to project's Mission, Environment, Applications and Lifetime (MEAL) should be developed and approved by Program/Project Managers with pertinent risks clearly identified, mitigated and accepted. ***(F-1, F-2, F-3, F-4, O-7)***

R-3. For critical or single point failure applications, strategically use MIL-SPEC or NPSL parts or part/system redundancy or both where it is resource-effective (e.g., cost, schedule, or space on the board/box). ***(F-1, F-7)***

NESC Recommendations: Verification when using COTS parts

R-4. COTS parts verification should be performed at part-, board- and/or system-level. If part-level verification is largely based on the COTS manufacturer's data, then the system should be tested 500-1,000 hours of accumulated test time, with the last 200 hours being failure free. ***(F-4, F-5, F-6, F-7, F-8, O-3, O-4, O-5, O-6, O-7)***

R-5. When using COTS parts, program/project should build multiple revisions of engineering units to start functional testing, environmental testing, qualification, and verification early in the design cycle so that any issue can be addressed to minimize the impact on system risk, cost, and schedule. ***(F-1b, F-3)***

NESC Recommendations: COTS parts selection, procurement and verification at part-level (I)

- R-6 When selecting COTS parts for spaceflight units, Circuit Designers should work with EEE Parts Engineers to follow a collection of best practices (Section 7.10.3): ***(F-5, F-6, O-1, O-2)***
- R-7 When purchasing COTS parts for spaceflight units, Project Procurement Organization and EEE Parts Engineers should follow a collection of best practices
- R-8 When verifying COTS parts at part-level, EEE Parts Engineers should follow a collection of best practices (Sections 7.2- through 7.9, 7.10.4): ***(F-4, F-5, F-6, F-7, F-8, O-3, O-4, O-5, O-6, O-7)***
- R-9 EEE Parts Engineers should perform obsolescence analysis on COTS parts to ensure projected part availability exceeds mission requirements over the duration of development or reuse for serviceable missions or GSE. ***(F-8, F10, F11, O-6)***

GSFC-specific addition*

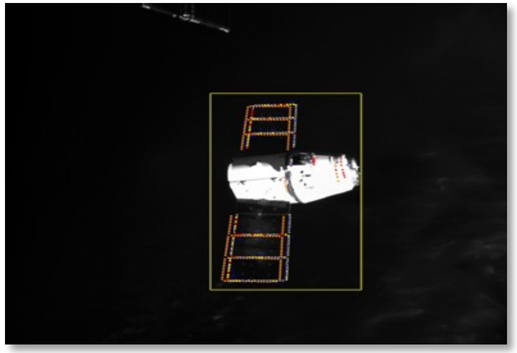
- GSFC has reviewed and discussed the study results
- GSFC has highly-successful and promising experience in intelligent use of COTS
- We have considered the study results in the context of our Center Risk Board
- GSFC is taking on a more aggressive, but intelligent, use of COTS that is reflected in a formal "opportunity"
- The following charts represent a GSFC-specific approach for intelligently phasing in COTS for more broad application, based on knowledge, substance, and understanding of risk

Example: Raven Payload*

Objective:

To advance the state-of-the-art in rendezvous and proximity operations (RPO) hardware and software by:

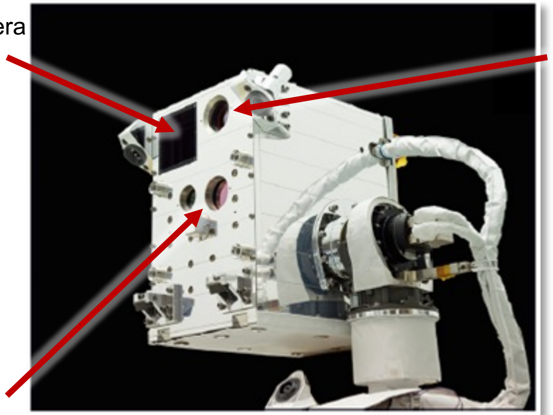
- Providing an orbital testbed for servicing-related relative navigation algorithms and software
- Demonstrating relative navigation to several visiting vehicles:
  - Progress
  - Soyuz
  - Cygnus
  - HTV
  - Dragon
- Demonstrating that both cooperative and non-cooperative rendezvous can be accomplished with a single similar sensor suite



Visible Camera

Infrared Camera

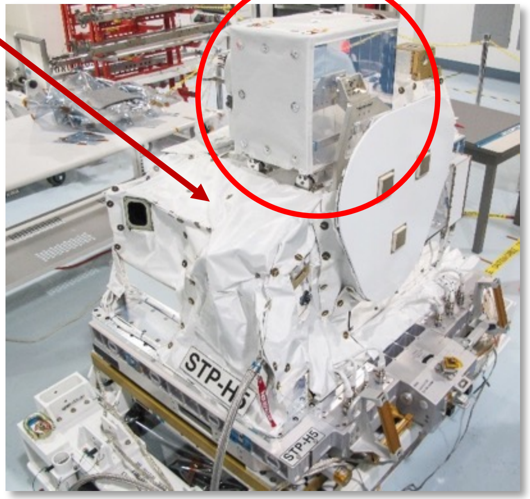
LIDAR



Raven
(Deployed Configuration)

$20M+ payload reliant on confidence in the SpaceCube computer, which in this case was pre-populated with 99% COTS Parts, and then thoroughly tested.

SpaceCube v2.0



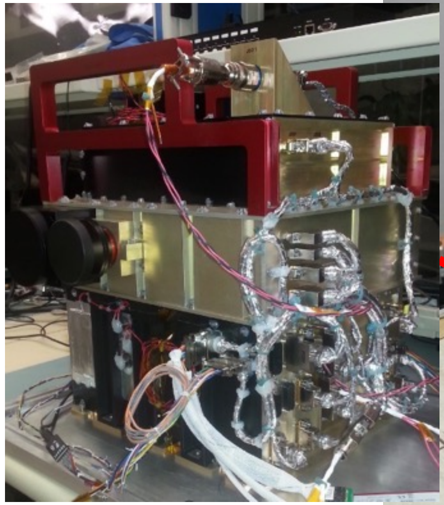
Raven installed on STP-H5
(Stowed Configuration)

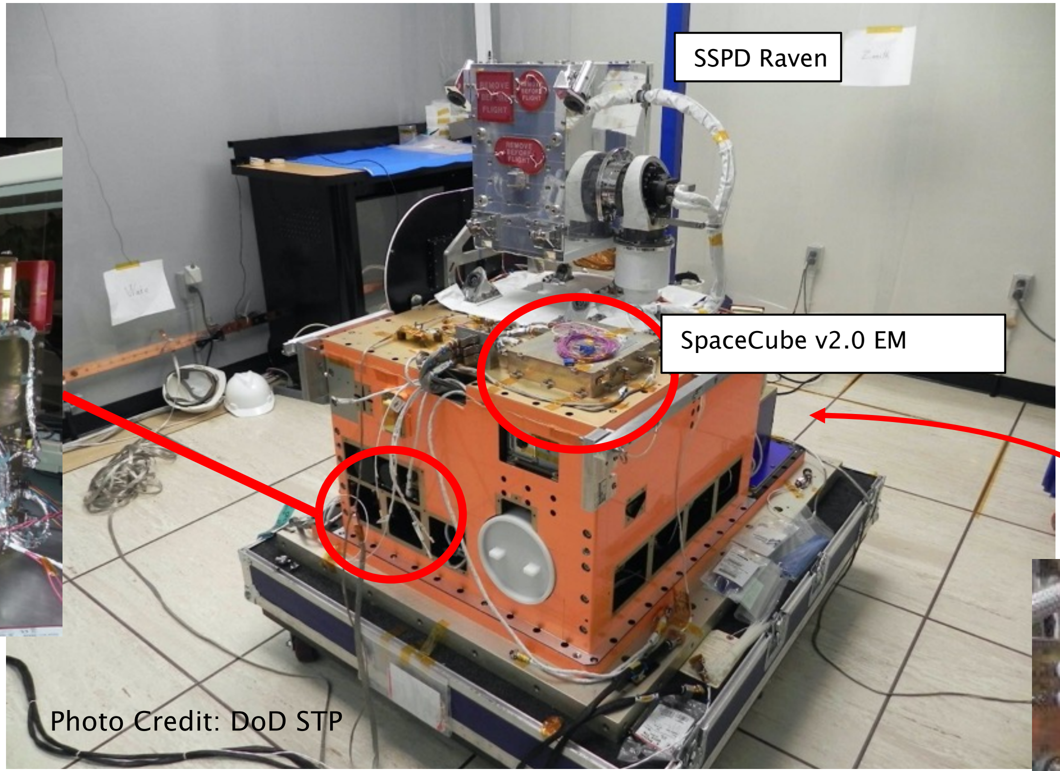
Cygnus Tracking

Example: STP-H5 ISS Payload*

26% COTS Parts

ISEM, SpaceCube Mini





99% COTS Parts

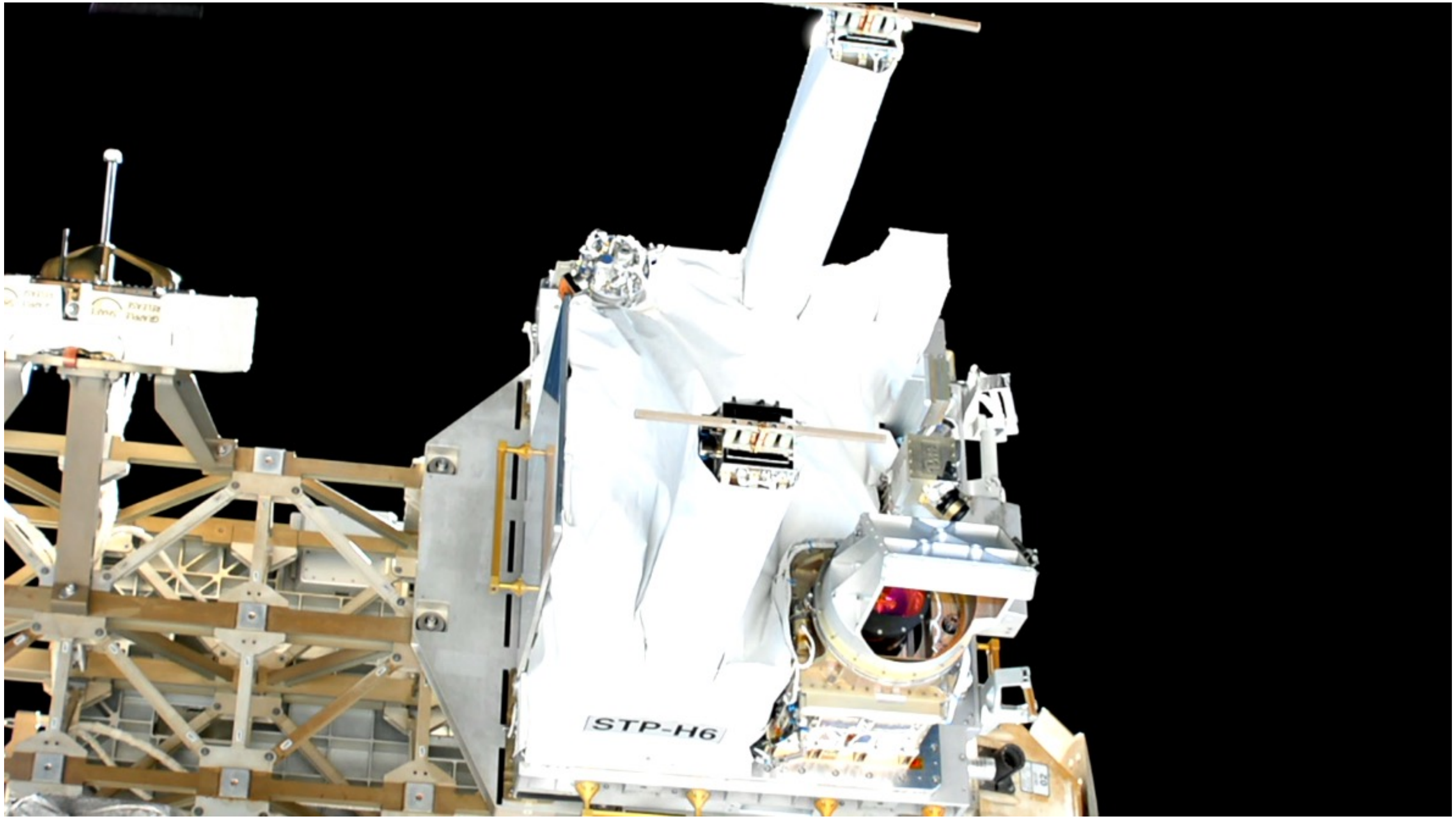
SpaceCube v1.0 CIB

1% COTS Parts

The Space Test Program-H5 (STP-H5) external payload, a complement of 13 unique experiments from seven government agencies, is integrated and flown under the management and direction of the Department of Defense's Space Test Program.

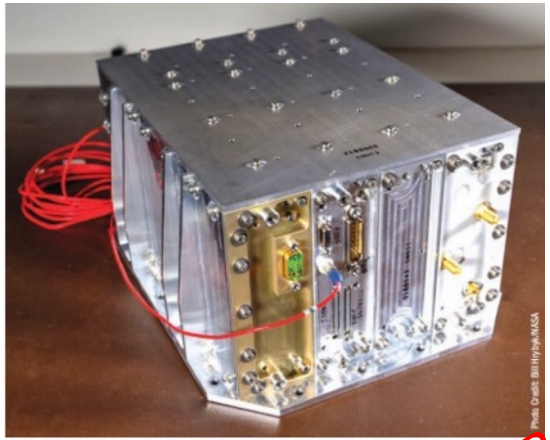
2/2017 – Current

Example: STP-H6 Payload*



99% COTS Parts

SpaceCube v2.0 NavCube



1% COTS Parts

SpaceCube v1.0 CIB

SpaceCube Time-on-orbit*

Project	Version	Part Req	BOM Count	Operation Months	Xilinx Quantity	COTS %	COTS Months
RNS	v1.0	2+	3700	0.0833333	4	1%	3.08333
MISSE-7	v1.0	N/A	3100	90	4	2%	5580
SMART	v1.5	N/A	1000	0.0333333	1	95%	31.6667
STP-H4 CIB	v1.0	N/A	1500	30	2	1%	450
STP-H4 ISE2.0	v2.0-EM	N/A	1250	30	3	98%	36750
STP-H5 CIB	v1.0	N/A	1500	46.933333	2	1%	704
STP-H5 ISEM	v2.0 Mini	N/A	1000	46.933333	1	26%	12202.7
STP-H5 Raven	v2.0-EM	N/A	1500	46.933333	3	99%	69696
RRM3	v2.0	N/A	1429	36.666667	2	65%	34057.8
STP-H6 CIB	v1.0	N/A	1500	31.833333	2	1%	477.5
STP-H6 GPS	v2.0	N/A	1157	31.833333	2	65%	23940.3
Restore-L Lidar	v2.0	3	2000		2	0%	N/A
STPSat6	v2.0 Mini	N/A	1500		1	98%	N/A

Totals	Units Flown	11
	Xilinx FPGAs	26
	Xilinx Device-Years	83
	Part Years	57213
	COTS Parts Years	15324

Also to note: We flew many COTS components on some of these projects:

- ISE2.0, SMART, and ISEM all flew COTS cameras that were ruggedized. SMART flew COTS SATA drives.
- Raven flew a $5 USB interface card to an IR sensor
- STP-H5 and -H6 have CHREC Space Processors (CSPs) that were 95% COTS components. See references for more info on CSP results (no failures to date)
- RRM3 suffered a failure (outside of SpaceCube) that may have involved a specific COTS part, but the part was used in a stressing condition that any part would eventually fail.
- NavCube Commercial vendor populated PWBs

Side-by-Side Comparison – Proper use of COTS*

Platform:
- SpaceCube v1.0

Parts:
- Level 1 and Level 2 Parts

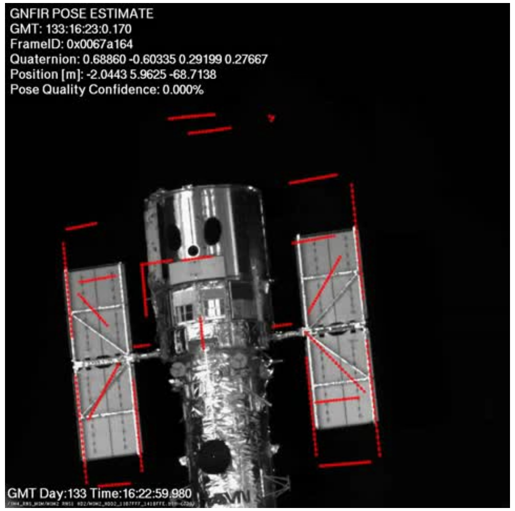
Application:
- Relative Navigation System
- Hubble Space Telescope Real-Time Tracking using 3x visual cameras

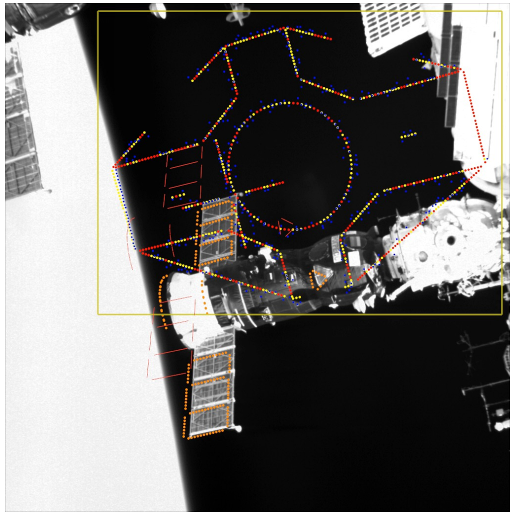
Identical Rigorous Design and Test Philosophy

Platform:
- SpaceCube v2.0

Parts:
- Commercially screened Parts (i.e. COTS)
- Ability to use any level of parts

Application:
- Raven Relative Proximity Ops
- ISS visiting vehicle real-time tracking using visual, Lidar, and IR instruments





Context for Risk in Parts*

COTS

- Parts with special features that are difficult to manufacture consistently (never available on MIL-SPEC)
  - e.g., extra-low ESR and ESL ceramic capacitors
- Parts used in brutal operating regimes
  - High-voltage (particularly > 3 kV)
  - Cryo
- Low volume and hand-produced parts
  - Lack a basis for reliability and often do not have optimized manufacturing processes
- Parts used in extremely sensitive (poor) designs (based on variability of parameters not in part spec)
- Parts used in applications in which the environment is unknown
- Parts from unknown or poor-performing vendors (no recent examples)
- No “hi-rel” or automotive parts available

MIL-SPEC

- **All risk-contexts for COTS*, plus**:
- Low-volume parts
- Lead time and costs can reduce system-testing resources
- Designed for old manufacturing processes and broad environments
- When used broadly, they can bring false hope and extensive problems may ensue
- Processes will miss new manufacturing flaws
- Performance and reliability not driven by the need to stay in business
- Performance limitations may lead to weak designs

NASA-screened COTS

- **All risk-contexts for COTS*, plus:**
- Parts are often overtested since MIL-SPEC testing regimes are not related to actual usage and parts are often not designed or optimized for such regimes
- False hope that screening is relevant to operation
- False hope that screening, testing, and qualification increase reliability or quality
- The prospect for burying a problem or reduced lifetime into a part by the “overtest by design”.

Note that the contexts for risk in COTS parts all arise from mission performance requirements that would be present no matter which parts approach is used, so they apply to all cases.

GSFC recommendations*

- Embrace the capabilities available in many classes of COTS parts
- Recognize the context for risk in COTS parts
  - ➢ Using them outside of their bounds/insufficient derating
  - ➢ Highly sensitive applications
    - High voltage
    - Cryo
  - ➢ Otherwise highly-sensitive parts
    - Commercial low ESL and low ESR ceramic caps
  - ➢ Hand-produced and very low volume parts
    - Questionable established reliability
  - ➢ Unproven manufacturers (no recent evidence of this being a problem)
- Follow Agency guidance – level 4 parts for Class D and below
- Consider COTS for Class C applications with proper context
  - ➢ Past vendor and component history
  - ➢ Fault-tolerant application
- Choose automotive or vendor hi-rel
  - ➢ Ask vendor for “zero defects” or “allowable DPPM” policy and policy for screening or testing every part
- Design circuits to be radiation tolerant (detailed recommendations in report) and fill gaps with testing or rad-hard parts
  - ➢ Radiation is another spec parameter that requires derating or characterizing and possibly accepting risk

Transition to COTS for existing designs?*

- How do you go from a successful Class B-developed product to a Class D application? (assuming D application is enveloped by the B environment, operations, and lifetime)
  - **Do not change parts**
  - For parts that were upscreened, use the same parts but do not do the screening or qualification
  - For MIL-SPEC parts, use the lowest grade MIL-SPEC parts that are readily available (not engineering/proto grade)
  - Do no require parts approvals unless parts must be changed due to lack of availability or obsolescence
  - Only use of a PCB is to evaluate changed parts
- How do you go from a successful Class D-developed product to a Class B application? (assuming B application is enveloped by the D environment, operations, lifetime)
  - **Do not change parts**
  - For high-volume parts (over 1M produced) from industry leading parts manufacturer (ILPM) from Hi-rel lines with ”zero-defects” policy, use parts as is
  - For others, establish a basis for acceptance (for those largely equivalent to pertinent MIL-SPEC parts, use standard Level 2 screening processes)
  - Do not require parts approval unless parts must be changed due to lack of availability or obsolescence
  - Validate radiation against environment for all parts, COTS, MIL, and NASA-screened COTS or radiation-tolerant design
- New S/C build recommendations:
  - Standard products (e.g., reused power supply CCAs) - follow first bullet
  - Standard spacecraft components- use inherited items process from GPR 8730.5 (applies to all classifications, not just D)
  - Other developments - use high-volume COTS from ILPM from hi-rel or automotive lines as first choice or any MIL-SPEC if available
  - When none available, use what is available and characterize risk based on context

Examples of intelligent usage of COTS*

- "Do no harm" – low-end 7120.5 Class D
  - Procure and use the parts you can afford
  - Do not change parts from existing design unless they are prohibitive
  - Good circuit design practices
    - Parts stress/sound derating
    - Radiation-tolerant design
- High-end Class D - Class C
  - If using existing, proven designs from any class, do not change or "screen-up" parts
  - Use automotive and vendor hi-rel whenever available
    - Use only parts that have 100% screening/electrical from vendor
    - Be cognizant of variability, especially wrt radiation/SEE
- Class A and B (future considerations)
  - Use vendor hi-rel from industry leading parts manufacturers
    - Use only parts that have 100% screening/electrical from vendor
  - Use high-volume when available, then automotive if no hi-rel
  - Do not change or "screen-up" parts from proven designs
  - Employ usage-focused screening practices for parts with risk context
    - Low-volume, hand-produced, etc
    - Unknown manufacturer
    - Stressing application (HV, cryo, etc)
    - Be cognizant of variability, especially wrt radiation/SEE

Emphasize radiation-tolerant design