SSC17-WK-03

Increasing Small Satellite Reliability- A Public-Private Initiative

Michael A. Johnson
NASA Goddard Space Flight Center
8800 Greenbelt Road, Greenbelt, MD 20771; 301.286.5386
Michael.A.Johnson@nasa.gov

Patricia Beauchamp, Harald Schone, Doug Sheldon
Jet Propulsion Laboratory, California Institute of Technology; 818-645-2479
Pbeaucha@jpl.nasa.gov

Linda Fuhrman
Massachusetts Institute of Technology/Lincoln Laboratory
244 Wood St, Lexington, MA 02421; 781.981.4949
Linda.fuhrman@ll.mit.edu

Erica Sullivan, Tom Fairbanks
Los Alamos National Laboratory
Los Alamos, NM 87545; 505.667.9219
eab@lanl.gov

Miquel Moe, Jesse Leitner
NASA Goddard Space Flight Center
Greenbelt Road, Greenbelt, MD 20771; 301.286.2281
miquel.a.moe@nasa.gov

ABSTRACT

At present, CubeSat components and buses are generally not appropriate for missions where significant risk of failure, or the inability to quantify risk or confidence, is acceptable. However, in the future we anticipate that CubeSats will be used for missions requiring reliability of 1-3 years for Earth-observing missions and even longer for Planetary, Heliophysics, and Astrophysics missions. Their growing potential utility is driving an interagency effort to improve and quantify CubeSat reliability, and more generally, small satellite mission risk. The Small Satellite Reliability Initiative (SSRI)—an ongoing activity with broad collaborative participation from civil, DoD, and commercial space systems providers and stakeholders—targets this challenge. The Initiative seeks to define implementable and broadly-accepted approaches to achieve reliability and acceptable risk postures associated with several SmallSat mission risk classes—from "do no harm" missions, to those associated with missions whose failure would result in loss or delay of key national objectives. These approaches will maintain, to the extent practical, cost efficiencies associated with small satellite missions and consider constraints associated with supply chain elements, as appropriate.

The SSRI addresses this challenge from two architectural levels—the mission- or system-level, and the component- or subsystem-level. The mission- or system-level scope targets assessment approaches that are efficient and effective, with mitigation strategies that facilitate resiliency to mission or system anomalies while the component- or subsystem-level scope addresses the challenge at lower architectural levels. The initiative does not limit strategies and approaches to proven and traditional methodologies, but is focused on fomenting thought on novel and innovative solutions.

This paper discusses the genesis of and drivers for this initiative, how the public-private collaboration is being executed, findings and recommendations derived to date, and next steps towards broadening small satellite mission potential.

MOTIVATION

At present, CubeSat components and buses are generally not appropriate for missions where significant risk of failure, or the inability to quantify risk or confidence, is acceptable. However, in the future we anticipate that CubeSats will be used for missions requiring reliability of 1-3 years for Earth missions and even longer for Planetary, Heliophysics, and Astrophysics missions. In addition, SmallSats could be developed using CubeSat components and subsystems but will not have the CubeSat form factor. Both CubeSats and SmallSats could then be used where their attributes enable or enhance mission objectives or provide other meaningful benefits—e.g. lower cost, increased coverage (spatial, temporal, spectral), agility, resiliency, etc.

Accordingly, the following discussion is not relevant only to CubeSats but also applies to small spacecraft that could benefit from CubeSat-derived systems, components, and development processes.

CUBESAT/SMALLSAT BENEFITS AND MISSION POTENTIAL

Over the last two decades, the advancements in microelectronics have allowed satellite developers to engineer ever greater capability into shrinking sizes, enabling more in-space capability for lower launch costs. We define Small Spacecraft (SmallSats) as spacecraft, enabled by ready access to space, that achieve meaningful missions and whose cost and schedule is not hampered by mission assurance practices, process, and architectures typical of billion dollar missions. Such spacecraft developments are enhanced by drastically scalable mission assurance enabled by new practices, process, and architectures that yield cost and schedule efficiencies. CubeSats, a type of small satellite comprising units measuring 10 cm x10 cm x10 cm and generally weighing less than 1kg, were first developed at Cal Poly and Stanford in the late 1990's as training tools for aerospace engineering students. Using commercial-off-the-shelf (COTS) parts, and mainly operating only in low earth orbit, these satellites were developed as short-term, high-risk experiments for educational purposes that fit into university budgets. However, the affordability and short development times of CubeSats were attractive to many in industry and government. This platform is now increasingly being considered for operational missions, for commercial use, for national security, and for advancing space science.

Many government organizations are considering using CubeSats to achieve mission objectives that otherwise would have been too expensive or not achievable. In particular, the following NASA applications are envisioned:

- For planetary missions, most applications consider one or more CubeSats to ride along the main spacecraft to augment the science return. CubeSats use the main spacecraft as a 'mothership' and are deployed for proximity operations or landers when this role is too risky or impractical for the main spacecraft. CubeSats/SmallSats are also envisioned to perform spatially- and temporally-distributed measurements through swarms or organized constellations. Using CubeSats in intentionally sacrificial missions, such as impactors, are another niche application under consideration for planetary bodies.

- In heliophysics, it has been said that "Most of the important phenomena involve simultaneous variations in space and time. In some cases, simultaneous measurements made at two well-chosen locations will provide unambiguous results. In other cases, it may be necessary to make simultaneous measurements at several hundred locations." CubeSats are an opportunity to more efficiently implement what had been done by large traditional spacecraft, through deploying many CubeSats in swarms or ordered constellations.

- Small astrophysics spacecraft can serve as pathfinders or calibration missions for flagship or probe missions. They can also comprise nodes in sensor networks that continuously monitor stars in deep space to detect and characterize exoplanets.

- For Earth-observing missions, development of complex, scientifically-valid instruments that fit the CubeSat form factor has grown exponentially over the last few years, covering almost all frequency bands within the electromagnetic band for a wide range of applications. The mission opportunities for LEO CubeSats/SmallSats are now being considered for many applications including monitoring storm evolution, capturing high spatial resolution mesoscale structures and phenomena that require large constellations that are not cost-effective to implement with traditional spacecraft.

While these applications target NASA-type missions there are other governmental agencies who also envision mission concepts impacted by these lower cost missions. In addition, SmallSats often serve as pathfinders for larger spaceflight missions, retiring the risk associated with flight systems and components that are later infused into these missions.

CUBESAT-SMALLSAT DEFICIENCIES

Reliability issues raise significant concerns when using CubeSats/SmallSats as *operational* systems. A comprehensive database of missions shows that more than 40 percent of CubeSats launched since 2000 failed to accomplish their objectives. While many of these systems were educational experiments or commercial prototypes, the overall market has been skeptical about whether CubeSats/SmallSats can be used reliably to accomplish critical operations, such as national security missions or deep space programs. The challenge for many developers is engineering a system consistent with targeted mission confidence levels while maintaining the reduced cost/schedule advantages associated with these platforms.

In the space community, we establish confidence in the development of any new space system based on decades of lessons learned, proven designs, established reliability histories of parts and components, involvement of experienced individuals, and through the use of cost/schedule margins in the development process to account for changing elements or unforeseen issues. In general, building spacecraft systems has benefited from significant resources used to cover development costs including numerous barriers of protection for safety and mission success, as well as sizable mass and volume on a launch vehicle to bring spacecraft into orbit. The advent of the CubeSat has provided the opportunity to change the paradigm created over many years when spacecraft have become ever larger and more complex.

The small size of the CubeSat has enabled multiple organizations, e.g., educational institutions at all levels, to produce complete CubeSats. This has led to new industries arising, opening the door to organizations that do not necessarily have the experience base to produce reliable spacecraft. In addition, time, money, and volumetric resources are not available with the same margins available to larger spacecraft. These aspects come together to drive a set of constraints on CubeSats that do not apply to larger spacecraft developments. For example, the use of most military specification (MIL-SPEC) parts, or parts screened to the MIL-SPEC levels, frequently are overly expensive, require too much time for delivery, and do not fit the profiles of the circuit card assemblies in CubeSat form factors. The components and assemblies that have been proven with widespread flight heritage in larger spacecraft, such as star trackers, inertial measurement units, reaction wheel assemblies, transceivers, etc. are well beyond the mass, volume, power, and cost constraints of a CubeSat/SmallSat. Hence, many components and subsystems are starting out without any reliability basis.

Fortunately, over the past decade, the international electronics industry has boomed, although the CubeSat community has yet to come to grips with how to take advantage of it. Furthermore, it has not yet been fully recognized that some of the conveniences built-in for larger spacecraft may not be appropriate for an excessively size-constrained application. For example, connectors have long been a means to trade space for modularity. However, even the small amounts of space required for connectors may be too much for the constraints of CubeSats. Past experiences on larger, low-risk missions have produced many lessons-learned on the integrity of connectors that steer many developers away from the few types of connectors that may be appropriate for a CubeSat. In many instances, wireless or other smart cabling approaches should be strongly considered where they may be appropriate; but this may require *different* analyses for electromagnetic interference.

The establishment of a CubeSat supply chain to produce parts and components helpful to broad CubeSat applications is in its infancy, as it is common to see very late deliveries and numerous products not functioning as specified, including many dead-on-arrival. Often the update cycle for electronic components is so rapid that establishing heritage is hardly even possible.

A major advantage offered by CubeSats/SmallSats in certain mission architectures is the ability to spread technical risk across multiple small satellites in a constellation. When a mission comprises multiple CubeSats, as opposed to a single high-reliability asset, the evaluation of success changes—the question becomes whether the constellation achieves its mission, not whether all parts of the system perform flawlessly. This represents a revolutionary change in the approach to system engineering for space systems, from traditional high-reliability large satellites designed to last for decades, to a “disposable” mentality where smaller satellites are engineered to perform a certain function for a short time, to address, in many cases, changing market needs.

More specifically, risk calculations for CubeSats systems need to take into account statistical reliability (i.e. some or most systems work well enough to achieve the mission, even though there are failures on some of the satellites) to determine how much risk a mission can tolerate, and then design to that risk. Therefore, the engineering development focuses on system resiliency to problems, and designing around failure modes, rather than trying to eliminate failures altogether. The system engineering requirements also vary depending on the requirements of the mission and how much risk that

mission can accept. For this reason, detailed best practices cannot be established for the CubeSat or SmallSat market as a whole, but only to the risk category each system is assigned based on its mission.

THE RELIABILITY INITIATIVE

The growing potential utility of CubeSats/SmallSats is driving an interagency effort to improve and quantify reliability, and more generally, small satellite mission risk. The initiative began with a conversation between engineers at NASA Goddard Space Flight Center (GSFC) and the Jet Propulsion Laboratory (JPL) on the need for small satellite technology appropriate for missions with high confidence expectations. Although systems and processes applied to large spacecraft could be applied to small platforms to achieve this outcome, such an approach would likely compromise characteristics associated with SmallSat-based missions—innovation, agility, and low cost relative to large. Accordingly, new approaches to address this challenge would be needed.

These discussions expanded to a team comprising interested persons from other government or government-like organizations. From this team was formed a sub-team of individuals with diverse and skilled perspectives. They realized government imposition could not derive solutions to this challenge, but instead, significant advancements could result from a collaborative public-private partnership engagement that exchanged needs, perspectives, expertise, and constraints.

Initial Recommended Approaches to Framing Solutions

A team with representatives from government and government-funded organizations was formed and tasked to address the following charge:

Recommend approaches to achieve reliability/risk tolerance associated with each mission risk class. Define and leverage novel component, subsystem, spacecraft, and mission-level risk mitigation strategies that maintain, to the extent practical, cost efficiencies associated with small satellite missions. Consider constraints associated with supply chain elements, as appropriate.

Team members worked on recommendations to address the charter in preparation for a Technology Interchange Meeting (TIM). The TIM was held at the California Institute of Technology on February 14th and 15th, 2017. The objective of the TIM was to reach agreement on a common language to help set expectations for CubeSat-SmallSat missions and expectations on the level of mission assurance for each classification. During the TIM, the subcommittee presented its findings and recommendations to date and solicited feedback and recommendations from attendees through splinter sessions and focused topic presentations. The TIM attendees included representatives from civil, DoD, academic, and commercial CubeSat providers and stakeholders.

Initial Recommendations

The initial recommendation defined risk levels and created a standard SmallSat/CubeSat risk classification nomenclature. The resulting nomenclature was similar to the NASA risk classification nomenclature. The subcommittee proposed activities required from the disciplines for each risk posture category, Alpha through Delta. The draft recommendations were formulated with the understanding that they were subject to change per recommendations made at the TIM.

TIM Findings

The TIM was structured in a way to promote thinking beyond proven and traditional methodologies. The group was tasked with identifying transformational solutions enabling the traditionally risk-adverse space community to adopt a new paradigm of space hardware engineering. The two-day event featured presentations of CubeSat science and operational mission drivers from various government organizations, select industry topic presentations including lessons learned, and presentations from the subcommittee regarding its findings and recommendations.

The mission assurance discussions were split into two categories. These categories were mission/system level assurance approaches and subsystem/component level assurance approaches. There were also presentations and discussions on future investments and knowledge sharing/collaboration.

The industry feedback on the government subcommittee's proposed risk classification system was that it was not very useful. Many of the TIM attendees stated that the system was too similar to NASA's traditional classification system and could therefore lead to significant constraints and burdens on a CubeSat mission. Many of the TIM attendees felt that by classifying a mission, it eliminated the flexibility needed to tailor mission assurance activities for specific subsystems and components. There was also disagreement regarding the number of bins needed for a CubeSat, i.e. three classes vs. four. Ultimately, there were two major recommendations regarding the subcommittee's recommended risk classification system. The first recommendation was that a confidence-based approach is preferred over a risk-based approach. Instead of characterizing risk, a CubeSat

mission should instead perform some level of assurance activities to achieve a threshold of confidence acceptable for their mission. Secondly, attendees stated that a "menu-style" approach is preferable when determining mission assurance activities for a CubeSat/SmallSat. Applying a menu-style approach to a CubeSat mission would facilitate a holistic approach to mission assurance where requirements are tailored based on trades at the mission or system level. With this model, a CubeSat mission may decide to perform high-confidence mission assurance activities in certain areas and medium- or low-confidence activities in other areas, based on which components of the CubeSat are absolutely required to meet mission performance requirements in space. Effectively, the mission would select its activities from a menu, and a determination of confidence-level would be made based on the activities performed and other contributing factors.

Other significant findings from the TIM and its related splinter sessions are as follows:

- Even in the fast-moving CubeSat market, it is essential to take a break between build cycles to capture lessons-learned and incorporate those lessons in the next design phase.

- Commercial EEE parts are appropriate for CubeSat missions with some caveats. When using such parts, care should be taken to ensure good thermal, mechanical, and electrical design to reduce parts stress, as well as robust board and system level testing to flesh out infant mortality issues.

- Developer should select parts with at least the temperature range necessary for the mission (with some margin), have a thermal engineer involved early in the process, and implement other thermal stress-reducing measures.

- Missions should electrically derate part stress levels where possible.

- Radiation effects can be a threat to mission success and must be seriously considered. In some cases, radiation testing of parts may be necessary and developers should consider implementing processes where radiation tolerance is achieved through design.

- In cases where higher reliability is needed for a particular part, developers should consider using automotive grade components; radiation effects still must be considered separately.

- A parts database containing radiation test results and other failure and anomaly information would be very useful to the CubeSat community and should be furnished by government organizations.

- The government should consider sponsoring radiation testing of selected CubeSat EEE parts and making the results available to the industry.

- The government should consider investing in the creation of a FAQ website where questions about CubeSat/SmallSat reliability can be asked and answered by subject matter experts.

- Software needs more attention and should be discussed in greater detail during a subsequent meeting.

- Routine clean room and safe-handling practices for electronics and flight hardware should be posted for vendors and academia to learn the hard-won lessons of the last few decades.

There was universal consensus that a parts database containing radiation test results and other failure and anomaly information would be very useful to the CubeSat community. The Air Force Research Laboratory (AFRL) has nearly completed development of its Space Parts on Orbit Now (SPOON) database. The SPOON database contains reliability information on previously-procured CubeSat subsystems. The SPOON database is not yet available for all users. While everyone agreed that database and information sharing would be useful, there are also some obstacles to overcome that must be addressed to reach this goal. It was agreed that this type of data sharing will require government leadership and moderation. Access control, source data anonymity, and data format standardization are examples of some of the challenges that must be worked through to establish the type of data sharing desired by the industry.

Success is best achieved when considering the processes to determine the reliability of a system. System-level testing processes include fully testing a system to failure, testing to characterize failure modes of critical subsystems, and methodically removing further testing of components that already have flight heritage. The participants suggested that to buy down risk and component-level test costs, CubeSat/SmallSat developers should fly new technologies on missions where that technology is not critical so that some flight data can be collected. This approach enables cyclical technology insertion by testing components and determining their failures modes when those components are not critical to mission success.

A representative from Planet at this meeting described Planet's success in embracing the "fly-fix-fly" approach

to technology insertion. Their conclusion was that on-orbit testing provided the best results and that despite the fact that on-orbit failures can be difficult to accept, "if you just keep going, eventually you get there".

It is clear that there is a need for a standard list of questions that facilitate discussion and engender transparency regarding a vendor product that has changed. The threshold for requalification could vary depending on the design, heritage, pedigree, and other factors. Therefore, it is important to know what changes have been made since the last qualification, what impacts those changes have on the system, and whether a vendor has confidence that a requalification should be performed. TIM attendees discussed testing at the board level instead of the part level when a requalification is performed and the possibility of performing analyses in lieu of requalification testing. When quantifying risks associated with design changes the TIM attendees largely recommended a 5X5 risk scale that is appropriate for CubeSats/SmallSats. It was also recommended to focus on qualitative data instead of quantitative data, and factor in heritage and pedigree.

A splinter topic question entitled "For each classification level, what is the appropriate level of testing (i.e. TVAC, Vibration, etc.) and what is the appropriate build and sparing policy" was also discussed but no firm conclusions were reached. The topic was deferred to the next meeting.

Much of the future investment discussion was about investing in data sharing. Software is another area requiring further discussion and future investment. Government-Off-the-Shelf (GOTS) Software, and NASA and DoD software licensing were some of the things discussed by the TIM attendees. It was agreed that software needs more attention and should be discussed in greater detail at the next TIM.

In conclusion, the TIM created an atmosphere of free and innovative idea exchange amongst its attendees. The team has taken all feedback into consideration and will continue to meet and work on a confidence-based approach for the different mission assurance disciplines needed to address CubeSat/SmallSat reliability. These recommendations will be documented in a paper that could ultimately be used as the basis for an industry CubeSat standard framework. Additional documentation on the TIM and findings from future activities can be accessed at the Small Satellite Virtual Institute website— https://www.nasa.gov/smallsat-institute/reliability-initiative.

A second CubeSat-SmallSat TIM is scheduled for October 2017 at NASA Headquarters. In parallel to the team's efforts, communication mechanisms and collaboration opportunities should be thoroughly explored for all areas where it is advantageous to the community (e.g. radiation and EEE parts database, failure and anomaly database, etc.).

POST TIM: REVISITING RELIABILITY APPROACHES FOR CUBESATS/SMALLSATS

Small satellite missions can generally be broken into higher-level (mission and system) and lower-level (component and subsystem) architectural elements. Depending on how these elements are combined and operated to accomplish the mission, reliability at one level may or may not relate directly to reliability at another level. For example, very reliable components (such as reaction wheels or radiation-tolerant piece-parts) don't guarantee reliability at the mission level if those elements are combined into an architecture with inherent flaws (undersized reaction wheels for maneuver control or electronics requiring more power than the vehicle can provide while maintaining the needed operational duty cycle). Missions involving constellations of satellites, for example, may be able to achieve overall high mission reliability even when individual vehicle or component reliability is not high. The breadth of potential missions, mission objectives, and architectures indicate that a "one-size-fits-all" approach to reliability is not likely to be efficient. A flexible approach to framing solutions for a particular mission is a more optimal approach.

For the next TIM, the team envisages proposing a spectrum of criteria and capabilities for both high-level (mission/system) and lower-level (component/subsystem) views of the mission, for which potential approaches to improve reliability are identified. The resulting matrices could provide a framework that the mission development teams can use to focus their critical needs and development areas, and then prioritize activities or design choices to make more effective plans for their particular mission. To illustrate, a few examples are provided below, and then explored further by walking through the possible selections two different missions might make.

At the Mission and System level, one can generally describe a variety of characteristics such as space environment (LEO, GTO, Deep Space) and configuration (single vehicle, constellation, mother/daughtership), and map these to a spectrum of mission criticality or potential reliability needs (national security critical need; operational mission; gap-filler; technology demonstration). These elements combined can help focus the overall reliability needs for the mission. Some LEO missions, for example, may have relatively frequent and inexpensive launch opportunities when compared to certain deep space missions, thus enabling an overall higher risk tolerance. Constellations may have overall higher risk tolerance for individual workmanship issues that may lead to individual vehicle failures, but very low risk tolerance for common failure modes that could cause the entire constellation to fail. A representative snapshot of this idea is provided in Table 1.

Table 1: A representative spectrum of risk tolerance as a function of the mission criticality and implementation approach

Risk Tolerance → **Mission Characteristics ↓**	**Very Low**	**Low**	**Moderate**	**High**	**Very High**
Mission Criticality	National Security; Operational	Operational; Primary Science	Gap Filler	Experimental; Technology Demo	Technology Demo; Teaching System
LEO Mission Life	5+ years	3-5 years	~1 year	Months	Days to weeks
Deep Space Mission Life	10+ years	5+ years	1-3 years	Months	Days
Single Satellite	Operational Mission	Data gathering	Gap Filler	Experiment	Technology Demonstration
Constellation (>10) Satellites	Common mode failures ruled out	High unit cost; limited "spare" vehicles		Multiple spare vehicles	Re-launch readily available
Flight Development Time	>5 years		~ 2 years		<12 months

Any particular mission concept is likely to map to multiple places on the risk tolerance spectrum depending on specific mission characteristic under consideration. For example, a notional mapping of a military mission could look like that in Table 2, and of a science instrument technology demonstration like that in Table 3.

Table 2: Mission characteristic risk tolerance for a hypothetical military mission

Risk Tolerance → Mission Characteristics ↓	Very Low	Low	Moderate	High	Very High
Mission Criticality	National Security; Operational	Operational; Primary Science	Gap Filler	Experimental; Technology Demonstration	Technology Demonstration; Teaching System
LEO Mission Life	5+ years	3-5 years	~1 year	Months	Days to weeks
Deep Space Mission Life	10+ years	5+ years	1-3 years	Months	Days
Single Satellite	Operational Mission	Data gathering	Gap Filler	Experiment	Technology Demonstration
Constellation (>10) Satellites	Common mode failures ruled out	High unit cost; limited "spare" vehicles		Multiple spare vehicles	Re-launch readily available
Flight System Development Time	>5 years		~ 2 years		<12 months

Table 3: Mission characteristic risk tolerance for a hypothetical science instrument technology demonstration mission

Risk Tolerance → Mission Characteristics ↓	Very Low	Low	Moderate	High	Very High
Mission Criticality	National Security; Operational	Operational; Primary Science	Gap Filler	Experimental; Technology Demonstration	Technology Demonstration; Teaching System
LEO Mission Life	5+ years	3-5 years	~1 year	Months	Days to weeks
Deep Space Mission Life	10+ years	5+ years	1-3 years	Months	Days
Single Satellite	Operational Mission	Data gathering	Gap Filler	Experiment	Technology Demonstration
Constellation (>10) Satellites	Common mode failures ruled out	High unit cost; limited "spare" vehicles		Multiple spare vehicles	Re-launch readily available
Flight System Development Time	>5 years	48 months	~ 2 years		<12 months

It is interesting to note that for these two hypothetical systems, the risk tolerance for the military mission covers the entire spectrum, depending on mission characteristics, while that for the science mission is heavily weighted towards a low-risk tolerance. These examples are provided to show that the implementation approach at the Component/ Subsystem level can vary widely, depending on how those elements map back to the mission characteristics. While mission criticality demands very low-risk tolerance for most military missions, the rapid system development time suggests that it *may* be appropriate to accept high risk in certain development areas.

At the Component/Subsystem level, the suggested approach is to develop a set of guidelines based on community best practices and heuristic data (when available) to guide prioritization of activities and processes to achieve the desired overall mission reliability. Items to be addressed can span the entire project lifecycle and include management approaches, design and analysis methodology, documentation and testing. As part of the SSRI, a preliminary set of items and associated lessons-learned are being compiled. A representative sample is shown in Table 4. The objective is to develop a guideline document with the vendors, updated when new data become available, to provide an effective planning and communication tool for mission development teams to identify their most critical areas and prioritize which activities or processes to pursue for the most cost- (or schedule-) effective solution for their mission.

Table 4: Potential examples of best practices to achieve desired specific reliability

Risk Tolerance → **Activity or Process ↓**	**Lower Risk Tolerance**	**← →**	**Higher Risk Tolerance**
Reviews	Formal SRR, PDR and CDR with external review board	← →	Internal informal reviews with key stakeholders
Drawings	Configuration managed drawings / CAD models with critical review and signoff	← →	Capture as-built configuration and key dimensions. Rudimentary CAD model recommended.
EEE Parts	Rad-hard or rad-tolerant parts in critical areas	← →	COTS parts; keep records of as-built
Thermal Cycling	Cycling at board, box, and full vehicle level	← →	At least four cycles at full vehicle level recommended
Environmental Test	Qual unit to validate design and Acceptance testing to validate workmanship	← →	As required by launch provider

FUTURE CONSIDERATIONS

The workshop has identified two critical elements that couldn't be resolved during the workshop. Many of the CubeSat providers felt that they have valuable experience in building reliable spacecraft and advocated to assume more of the development and assurance risk. Further, communicating the proper risk posture for SmallSats and CubeSats couldn't be achieved by merely adopting the NASA risk classes as defined in NASA Procedural Requirements (NPR) 8705.4 (Risk Classification Guidelines for NASA Payloads) for missions governed by NPR 7120.5 (NASA Space Flight Program and Project Management Requirements), as the missions had requirements that were too diverse to fit the large application and risk spectrum. The consolidated community realized that it is possible to negotiate a risk posture and determine who is carrying the risk as long as all contributing risk elements are disclosed, all assumptions are identified, and a logical construct is built to prove that all listed risk elements and assumptions will completely describe the final system.

Such an approach can be derived from the concept of a "Safety Case." A Safety Case is a structured argument, supported by evidence, intended to justify that a system is acceptably safe for a specific application in a specific operating environment.[1] Developed over several decades in the UK, they are in widespread use in Europe and elsewhere as the means to organize and present the rigorous argument for the adequate safety of

major industrial installations (e.g., transportation systems, chemical plants, oil platforms, nuclear plants, weapons systems).

The need for sophisticated systems approaches highlights the contradictions and challenges that CubeSats and SmallSats present. The rapid advances in the capability of commercial electronics and modern highly-optimized manufacturing processes result in highly-integrated and engineered systems being made available to mass markets with a concomitant decrease in cost. Such a decrease in overall space flight costs are only now beginning to be realized but this presents unique challenges coupled with the extreme and often unforgiving environmental conditions that space flight operations entail. Inexpensive electronics do not imply an inexpensive or possibly limited rigorous approach to risk mitigation and assurance. It should be noted that the interdependencies and system interactions, requirements, and overall complexity of spacecraft operation regardless of physical size, demand a sensible risk approach. Leveraging modern simulation and analytical tools developed for other similarly complex and often high financial risk industries is a logical and reasonable approach that can quickly provide 'value added' robustness to the overall decision and review processes for CubeSat/SmallSat missions.

Miniaturized satellite systems pose an additional challenge—not only is the system tied to unique operational and environmental constraints, but much of the contributing component testing data does not exist. Therefore, tracing requirements directly to system performance from the design through operational testing is extremely difficult due to the large operational space that precludes exhaustive testing for the cost envelopes of these missions.

Formal Assurance Cases, such as those provided through the use of the Goal Structuring Notation (GSN), provide the framework to do this. We see them being used elsewhere to assure the safety of UAVs, a burgeoning use of autonomy in a terrestrial arena.[2]

Since the workshop concluded, members of the reliability team have taken the challenge of adapting the use of assurance cases to a test case of a SmallSat space mission and developed the construct prior to the contract award. It is expected that this will make will make it possible to clearly identify mission risk drivers and lay the foundation to negotiate risk.

This initiative is an ongoing process, whereby we hope to come to an approach acceptable to all participants. Along with the upcoming 2nd TIM in October, there is a Mission Assurance Improvement Workshop (MAIW) to explore and document best practices and craft a common approach to mission assurance for the U.S. space program. The MAIW is a community of practice dedicated to the development and promulgation of proven scientific, engineering, quality, and program management practices related to the U.S. space program's mission success.[3]

Acknowledgments

A special thank you to Elizabeth Klein-Lebbink from The Aerospace Corporation for her contribution to this activity and to others who have lent their perspectives. The authors recognize we did not exclusively derive the findings reported in this paper. They are informed by the collective work of participants of the SmallSat Reliability TIM.

References

1. Defence Standard 00-56 Issue 4 (Part 1): Safety Management Requirements for Defence Systems. UK Ministry of Defence. p. 17.
2. "Perspective on software safety case development for unmanned aircraft," E. Denny, G. Pai & I. Habli, IEEE/IFIP Inter. Conf. on Dependable Systems and Networks, 2012; "Understanding and Evaluating Assurance Cases," Rushby, at al., NASA CR2015-218802, LRC, SEP 2015.
3. http://www.aerospace.org/publications/getting-it-right/mission-assurance-improvement-workshop-product-list/