[Paper Number]

The Small Satellite Reliability Initiative: A Public-Private Effort Addressing SmallSat Mission Confidence

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

Patricia Beauchamp, Harald Schone
Jet Propulsion Laboratory California Institute of Technology;
4800 Oak Grove Drive, Pasadena, CA 91109; 818-645-2479
PBeaucha@jpl.nasa.gov

Catherine Venturini
The Aerospace Corporation
El Segundo, CA 90245; 310-336-5923
Catherine.C.Venturini@aero.org

Lee Jasper
Space Dynamics Laboratory- Air Force Research Laboratory
1851 Charlene Dr. Kirtland AFB, NM 87117; 303.204.1156
Lee.Jasper@sdl.usu.edu

Robbie Robertson
Cubic Aerospace
12110 Sunset Hills Road, Suite C4, Reston, VA 20190; 571.299.6977
RobbieR@cubicaerospace.com

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

Florence Tan
NASA Headquarters
300 E St. SW, Washington, DC, 20546; 202.358.0058
Florence.W.Tan@nasa.gov

ABSTRACT

Presently, most CubeSat components and buses are generally not appropriate for missions where significant or indeterminate risk of failure is unacceptable. This has precluded their use in many cases where their attributes could otherwise enable or enhance mission objectives. However, in the future, CubeSats and SmallSats, which deviate from CubeSat form factors but often incorporate CubeSat components and subsystems, will address challenges that many presently consider to be beyond the platform's capabilities. This growing potential utility, combined with the limited volume of successful CubeSat flight heritage, is driving an interagency effort to improve small satellite mission confidence.

The Small Satellite Reliability Initiative (SSRI)—an activity with broad participation from civil, DoD, and commercial space systems providers and stakeholders—has been targeting this challenge. This paper will update the community on how the public-private collaboration is being executed. It will discuss mission confidence approaches considered and defined to date, why and how they were derived, and next steps the team will implement to broaden SmallSat mission potential.

SSRI MOTIVATION

Presently, CubeSat components and buses are generally not appropriate for missions where significant or indeterminate risk of failure is unacceptable. This has precluded their use where their attributes could otherwise enable or enhance mission objectives or provide other meaningful benefits (e.g., lower cost, increased spatial, temporal, and spectral coverage, agility, resiliency;, etc.). Historically, this has not been an issue since it was understood and accepted that "high risk" and "CubeSat" were largely synonymous and expectations were set accordingly.

The landscape is changing, however. In a NASA context, numerous CubeSat and SmallSat missions—small satellites that deviate from CubeSat form factors but often incorporate CubeSat components and subsystems—have been defined, are in development, or are deployed. These include scientific missions requiring 1-3 years of reliable operation in Earth Orbit, missions to Mars and Venus, asteroids and comets. There are also astrophysics concepts that seek exoplanets or missing matter by mapping the distribution of hot gases in the Milky Way, and CubeSat constellations that operate as a synthetic radio telescope probing solar energetic particle acceleration and release to address key Heliophysics questions. Other governmental agencies have also formulated concepts that require mission success; interest in these platforms is not unique to NASA.

These developments are evidence of the growing utility of these platforms and are driving a public-private effort to improve CubeSat and more generally, small satellite mission confidence, while preserving cost efficiencies of these platforms.

INITIATIVE OBJECTIVES

The Small Satellite Reliability Initiative (SSRI) has been targeting the SmallSat mission confidence challenge. SSRI with broad participation from civil, DoD, and commercial space systems providers and stakeholders has made significant progress towards defining and documenting a range of best practices and design/development guidelines—from those aligned with "do no harm" missions, to those whose failure would result in loss or delay of key national objectives. The effort approaches the challenge from multiple perspectives—from a high level that considers top-level mission architecture and objectives, to a lower level that considers component/ subsystem issues.

SSRI considers several approaches to the challenge. These approaches and questions being addressed are as follows:

- **Best Practices and Design/Development Guidelines—**What design/development guidance and best practices are consistent with confidence levels ranging from "do no harm" missions to those whose failure would result in loss or delay of key national objectives? How should we "package" these guidelines so that they have the greatest utility and impact to the broad SmallSat community?

- **Lessons Learned—**What should we learn from SmallSat missions that have flown and from missions in development to inform the success of future missions?

- **Knowledge Sharing—** The pace of SmallSat mission capabilities advancement will be informed by how broadly the community shares knowledge. What information and resources should the SmallSat community exchange to increase mission success and reduce overall development costs? How do we grow and nurture a community that exhibits a willingness to share such knowledge more widely than historically demonstrated? How do we disseminate it to where it is needed, when it is needed—to new entrants and established entrants alike? What is the Government's role in facilitating such sharing?

- **Model-based Approaches to Mission Confidence**—How can we harness and apply the potential effectiveness and efficiencies associated with model-based approaches to small satellite mission confidence? How do we inform the development of these tools such that their learning curve and user efficiency do not raise user entry and utilization barriers.

SUMMARY OF PREVIOUS FINDINGS

The paper *Increasing Small Satellite Reliability- A Public-Private Initiative*[1] documented community recommendations from Technical Interchange Meeting-1 (TIM-1) convened at the California Institute of Technology in February, 2017. The first recommendation was that a confidence-based approach is preferred over a Class A-D risk-based approach. Instead of characterizing risk, a SmallSat mission should instead perform some level of assurance activities to achieve a threshold of confidence acceptable for their mission.

Secondly, attendees recommended a "menu-style" approach to inform the assurance activities appropriate for a given CubeSat/SmallSat mission. This 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 SmallSat 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 SmallSat 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.

These recommendations have led to a focus on several approaches to mission confidence—

- Best Practices and Design/Development Guidelines
- Lessons Learned
- Knowledge Sharing
- Model-Based Approaches

A discussion of these approaches follows.

2018 PROGRESS: INTERIM BEST PRACTICES AND DESIGN / DEVELOPMENT GUIDELINES

There have been two SSRI Technical Interchange Meetings (TIMs) since the first one. TIM-2 was held in October 2017 to discuss reliability topics (and in some cases the broader scope of mission assurance) as defined in a report titled "Mission Assurance Guidelines for A-D Mission Risk Classes" under section A5-3 Matrix - Reliability.[2] The agenda[3] for this meeting can be found and a summary[4] of the meeting are publicly available.

As a result of these TIMs, a working group (WG) was formed. This group comprises about 30 members from across industry, government, and academia. Using the 35 reliability topics defined by the Aerospace Corporation's Technical Operating Report (TOR), the WG researched each topic and documented best practices, references, and key questions that would help someone identify how and when a topic should be used in the development and operations of small satellites.

This WG also focused on defining a method for distributing the information to the small satellite community. The current archiecture focuses on a web-based data set that uses a searchable database of the information and resources collected so that users can have more of a "one-stop-shop" for what Reliability means and how to apply it to small satellites. Further the web-based architecture will have more of a guided, interactive tool that could be used to help users through which reliability topics are the greatest return on time and cost investment to improve mission assurance. This tool asks a basic set of questions regarding the mission of interest and then offers guidance on which specific practices that inform mission confidence should be used, or not used. While still a work in progress, key questions are:

- What is the mission architecture and how does this inform practices for *missions such as:*
  - A large Low Earth Orbit (LEO)/Medium Earth Orbit (MEO) Constellation
  - A Geostationary Earth Orbit (GEO) satellite with lifetime of $\leq$ 5 years in orbit
  - A mission beyond GEO
  - A LEO mission with 1-2 satellites and lifetime < 1 year
  - A LEO mission with 1-2 satellites and lifetime > 1 year
- What are the key practices that reduce mission risk and increase mission assurance?
- Are there any specific mission or hardware drivers that weight some practices higher/lower impact?
  - What are the key technical challenges and risks?
  - Should higher risk elements receive more focus?
  - How much program risk is acceptable?

This work will help organize and better define "heritage" processes and practices (i.e. the 35 reliability topics). The group also collected best practices from the 35 topics plus a small subset of past, present, and future missions. These both inform, and help expand, the scope of the best practices to be done.

Summary of Top Confidence Building Activities

During the most recent Technical Interchange Meeting (TIM-3) following the CubeSat Developers Workshop in May 2018, the attendees voted on the top activities (from the 35 topics) that yield greatest increase in confidence. This was based upon experience/opinion of a variety of people from industry (7), academia (9), and government (11). These top activities include *engineering the system for higher confidence*, *design review and analysis*, *radiation testing*, and *software reliability*. The key practices are further detailed in the next subsections since they were identified by the larger team as key best practices. Note that findings are interim; the best practice effort is ongoing.

Engineering the System for Higher Confidence was voted by the TIM-3 attendees as the topic area they found most useful for increasing SmallSat reliability. The topic, as explored by the WG, focused on identifying perspectives that should be considered within the SmallSat systems engineering process that can enhance mission and system resiliency and ensure the entire system is appropriately defined for the mission. Cost, schedule, and risk posture of the mission are a few of the factors identified that can significantly impact the systems engineering methods and processes that a SmallSat employs. Trades must be performed by each mission to determine the most feasible approach. Some of the Systems Development Life Cycle (SDLC) models and methods identified by the SSRI WG are listed below.

- Waterfall Model[5]
- V Model[6]
- Evolutionary Prototyping Model[7]
- Spiral Method (SDM)[8]
- Interative and Incremental Method[9]
- Agile Development[10]

Many of the models and methodologies listed above have been proven on traditional mission architectures and software engineering. They can be broad and conservative in nature. They were designed to cover a wide range of mission applications. For SmallSats it is extremely important to understand what mission specific systems engineering activities and methodologies add the most value given resource constraints. One idea that has the potential to achieve this is Model Based Systems Engineering (MBSE) and Model Based Mission Assurance (MBMA)[11]. Effective MBSE and MBMA requires intimate knowledge and understanding of a particular mission architecture and application. If modeled with high fidelity MBSE and MBMA can provide a SmallSat project with a value added understanding of what systems engineering activities should be pursued. The challenge associated with MBSE and MBMA, at the moment, is the tradeoff in overhead to perform and maintain the modeling versus performing the traditional systems engineering activities. This is something that is being explored and must be addressed in order for MBSE and MBMA to be useful to this class of missions.

Small satellite missions often have unique cost- or capability-driven constraints. These constraints should inform a mission architecture that mitigate their impacts. Consider for example, the ground segment and command/data bandwidth. Cost and capability may constrain operators' ability to monitor and control in-space assets. Such an impact can be mitigated by migrating targeted functions that are typically executed on the ground—such as fault detection and recovery—to space. Such approaches to "engineering the system" for resiliency, are critical to the achieving target levels of mission confidence. The WG expects many novel approaches are yet to be conceived.

Design review and analysis is another topic that the TIM-3 attendees found to be useful. Interim guidelines summarize standard design reviews, illustrate which reviews are often employed at the mission and subsystem level of a program, and describe best practices for effective reviews. Similar to the systems engineering section, the SSRI WG found that SmallSat design reviews may be combined or eliminated depending on the project budget, schedule, and risk posture. For example, very small spacecraft (e.g. CubeSats) might not need a set of separate, formal Subsystem-level reviews. Especially when a subsystem (e.g. power or the attitude determination and control system (ADCS)) is being procured as a commodity item and has already been delivered and/or flown for other customers. The NASA Systems Engineering Handbook (NASA SP-2016-6105) was used as a reference to define the different reviews a SmallSat mission may consider and when they are applicable. NASA Systems Engineering Processes and Requirements (NPR-7123-001B) was also referenced to show when reviews are typically held throughout the project life cycle and the product maturity goals for the different reviews.

Radiation testing was tied for second place with design review and analysis for topics that the TIM-3 attendees found most useful. Radiation testing was likely ranked high by attendees due to the number of electronic subsystem designers present. An overview of radiation sources present in the space environment (e.g. solar particles), types of radiation effects (e.g. single event effects (SEE)), and radiation tests with best practices were provided in this section. In summary, it's important for SmallSats to understand the susceptibilities of the EEE parts they have selected, whether though test, analysis, or historical knowledge of the part or its fabrication and design process.

The WG has spent significant time investigating these topics and has queried numerous sources to derive interim findings in each area. However, the WG has recognized that significant work remains to organize the information that has been collected and tailor best practices to small satellites.

Software Reliability. In-space software will greatly inform mission confidence—either through practices that yield reliable software, or through practices that can mitigate the impact of system failures and anomalies. The following recommendations largely address the former.

The WG identified and addressed many elements that improve software reliability both from best practices and established processes. Several specific definitions are used relative to software. "Reliable software" is robust and fault tolerant, has very few, if any, bugs and has a long mean time between errors. When an error occurs, it is able to handle off-nominal conditions, invalid inputs, unforeseen events, and varied operational scenarios, handling the error and recovering gracefully. Reliable software is a subset of quality software. "Quality software" typically considers functionality, usability, efficiency, maintainability, portability, scalability, and reliability.

The following discussion summarizes best practices on how to achieve reliable software, organized into three major elements:

- Management (organization/staff, managing Information Technology (IT))
- Process (development methodology, testing)
- Implementation and Coding Techniques (watch dog timer use, exception handling)

Management- Software Reliability

Mentoring: Pair senior experienced programmers to mentor to junior programmers

Embed software engineers with stakeholders*:* Embed software engineers with hardware engineers and scientists for new research and development. Currently, many organizations do not do this. For example, NASA uses software development groups that are often physically separated from the hardware and instrument developers. One of the advantages of many small satellite teams is there is a potential for greater hands-on feedback between all parties.

Process- Software Reliability

The software development process has to match the underlying project and be cognizant of the stakeholder's expectations. It should address issues such as how is the software going to work with the hardware? What is the operational scenario? What data are expected to be produced? Early in a project, structural patterns are more useful than requirements in developing the basic architecture for a software system. One key practice is to conceptualize the software and see how it interacts with all other elements of the mission. There should be an understanding of the concept of operations, characteristics of components, the scheme of the software, the use cases, operational scenarios, and the hardware interfaces. Development of a hardware-software interface control document (ICD) can be useful for early software design. This is a more useful mental model for early software development than merely listing the requirements.

Understand what are hard versus soft requirements: Programmers need to have a sense of the types of things that can change during development and what is inflexible. Key contributions to requirement definition include:

- Conducting trade studies as necessary
- Including hardware testability into software requirements
- Partitioning ground software functions and flight software functions early
- Planning for software development targets/platforms that precede flight hardware
- Planning how to upgrade/patch flight software
- Making fault tolerance and error handling part of the software architecture from the beginning

Plan a robust testing program: Set up a testing schedule and understand what configuration of component units are needed to perform the tests planned. Coordinate with management to plan appropriate units of hardware builds. Test as early as possible. Perform software assisted component end-to-end testing as soon as available and aim for end-to-end flat-sat tests as soon as possible. Plan to use simulators and dummy loads for testing to increase fidelity of tests. Institute an *independent* testing program; the software programmer should be different than the tester.

Implementation- Software Reliability

Design the system architecture for test and operation: Start early conversations between hardware and software engineers. Both sides must understand the hardware/software interfaces and requirements. Software requirements drive hardware design and vice versa. Design the system such that if failure or fault occurs, the root cause can be derived from the telemetry and science data. The system should be configurable such that telemetry can be commanded to vary collection of type and frequency of telemetry data if necessary.

Use of timeouts*:* Liberal use of watch dog time outs will prevent software from hanging and provide a "safety valve" for the software to trap and handle errors.

Exception handling*:* Think through faults and contingency cases. Have event handlers that detect errors within software. Create syntax checking code. Have a process in software that consistently detects, handles, and responds to anomalous conditions in a safe manner

Use of good programming practices*:* Minimize scope of variables, have simple testable modules and minimize parameters allowed for unit testing, design and write code to minimize paths such that full path test is that is not onerous, practice modularity with small subroutines; break the work down so that they are easily testable, trackable, understandable, strictly use revision control system, and strictly employ a bug tracking system.

Software repository: Build a repository of tested code based on standard hardware for reuse. Given hardware always changes, build a layer of software that is designed to be configurable for new hardware e.g., NASA cFE's "OS Abstraction Layer"

Testing: Bake-in the testing into the code; in other words, when developing new modules, think and write the test code. Coordinate the test suite – have a program that can test the software as you run. Automate suite testing and unit testing to the extent practical. "Unit testing" is testing individual modules separate from each other. It requires designing well written modules with carefully designed and controlled interfaces for minimal external effect. Poor code might have large unwieldy modules that cannot easily be tested independently.

There are many facets to software reliability and programs can utilize some or all of the above practices. Many of the implementation practices and testing practices should be prioritized as they are, often, highest return-on-investment.

LESSONS LEARNED

Small satellite missions rarely fit into traditional reliability classifications; therefore, design and reliability practices vary more than those of traditional space programs. SSRI technical interchange meetings have included lessons learned presentations by leaders of SmallSat missions that have addressed a diverse set of missions, including a 3U CubeSat RF technology demonstrator, an ESPA class imaging satellite, a MicroSat LEO Earth science constellation, and Lunar 6U CubeSat. Lessons learned from these missions provide important guidance for future SmallSat teams. Many of the findings from SSRI's 2018 meetings were originally identified in SSRI TIM-1 in February 2017, which are summarized in the bulleted list in the "TIM Findings" section of Johnson et al., 2017[12]. In this section, additional lessons learned from the more recent TIMs are described.

Subsystem procurement and EEE part selection. For SmallSat missions, following existing standards is not typically practical in selection of EEE parts or subsystems. As a result, a common thread in the lessons learned shared through the SSRI has been subsystem procurement and EEE part selection. At the EEE part level, use of commercial and automotive grade components is key to keeping costs low. However, each part should have a reliability "story" that addresses the risks associated with flying parts that are not space qualified and screened. This story should provide answers for thermal, structural, and radiation performance in the expected environment(s) via testing, flight heritage, or analysis. In many cases, this story will not satisfy stated mission goals or will simply acknowledge that the reliability is unknown – this is still extremely valuable. Identifying and documenting these risks allows for feedback into the design process. When using EEE part test data, it is essential to consider the risk of design changes and lot-to-lot variations in commercial/automotive grade parts that are not manufacturer qualified to the target environment(s) (e.g. radiation, thermal). This risk can perhaps be mitigated via derating relative to the test results.

Parts Reliability. The level of subsystem design and manufacturing variability currently in the SmallSat market provides additional challenges to parts selection process. To mitigate the reliability uncertainty caused by the lack of strict design, manufacturing, test, and analysis requirements it is essential for SmallSat design teams to communicate with vendors. Such engagement will help the development team identify the highest risk sub-systems or weakest link in the typically single string system. This triage of risk allows the team to focus additional effort to minimize performance-loss, efficiency-loss, and any budget on the areas most likely to fail

Fault Recovery and On-Orbit Reconfigurability. Design and planning for fault recovery and on-orbit reconfigurability was found by several SmallSat missions to be essential for mission success. Downlink of housekeeping/state-of-health telemetry and having a representative flatsat is key to on-orbit failure recovery, resolution, and mitigation. An ability to accommodate software updates should inform the designs of the spacecraft communications subsystem and ground stations; uplink capability has been a challenge for many missions.

Management. Establishing a SmallSat team and managing the design process was found to be an important element of an efficient yet reliable mission. SmallSat mission leaders found that small but experienced teams with reduced administrative burdens were ideal. The best practices and judgement of an experienced team can be used to reduce risk when the level of analysis, test, and review associated with traditional programs is not possible or practical with SmallSat budget and schedule constraints.

Design guidelines and best practices applied by SmallSat teams. The unique constraints of SmallSat design leads to unique hardware design challenges, solutions, and failures. This leads us to another common thread in lessons learned shared through the SSRI: specific design guidelines and best practices applied by SmallSat design teams. In this respect, the output is the following list of somewhat disparate guidelines/best practices that were either found valuable to success by a particular mission, or that would have prevented an on-orbit anomaly or failure:

- Increase amount of telemetry collected on-board and avoid use of inferred information. The expanding use of satellite-to-satellite relay greatly increases the bandwidth possible.
- Avoid scaling "big space" reliability practices to small satellites but instead scale small satellites to higher levels of detail to address critical elements and tall poles.
- Vehicles need to have the ability to hard reset the computer and other elements to properly clear Single Event Effects (SEEs).
  - Ensure this capability is independent of the flight computer
- Vehicles need to have ability to reprogram/update software.
  - Do not discount the need for uplink bandwidth. Data volumes can be large when updating flight software anomalies.

KNOWLEDGE SHARING

Improved avenues for knowledge sharing have the potential to benefit all members of the SmallSat community: government, industry, and academia. Knowledge sharing avenues addressed to date by the SSRI cover three distinct areas: parts, subsystems, and missions.

Parts

Sharing part-level test data has been traditionally facilitated by government organizations and part manufacturers. These reports allow for subsystem developers to minimize risk while designing with commercial parts when possible and practical given a radiation environment and risk posture. These EEE part radiation reports are most readily available on NASA (JPL and GSFC) and ESA online databases, with additional test data available through various journals, conference proceedings (e.g. NSREC), and other places. Unfortunately, the data are spread in multiple locations and in different formats. Furthermore these databases are often years out of date with respect to the test data that have been collected and analyzed. The NASA Small Spacecraft System Virtual Institute is currently developing a federated radiation database portal to allow access to all of the key databases from one site and search/browse page.

When companies invest in part-levels radiation testing, the cost and competitive advantage provided by the testing and analysis usually precludes them from sharing with the community. SSRI discussions led to a few knowledge sharing concepts that can broadly benefit companies. One concept involves the formation of a consortium where all entities would, under a mutual non-disclosure agreement (MNDA), pool their EEE part radiation test data. However, it would be very challenging to ensure that all members contribute their part to the pool of data. A simpler concept involves an online board where entities register and share what data they have or what they are looking for (with whatever level of detail they are comfortable sharing). This would allow users to search the postings that align with their needs and follow up outside of the system to arrange trades or purchases of test data.

Subsystems

Subsystem level data sharing is currently underway through the Space Parts on Orbit Now (SPOON) database developed by the Air Force Research Laboratory (AFRL); however, access is still limited. There are efforts underway to make it accessible to a wider community (see Johnson et al., 2017[13] for more details). SPOON currently hosts datasheets and specifications for SmallSat subsystems. In the future, subsystem integrators will be able to to report and share failures or more minor issues in the database. This feedback will help vendors improve their designs and assist others with product selection and integration.

Missions

Statistics on mission success/failure and other details that have been shown to contribute to mission success have been analyzed. This work (e.g. Swartwout and Jayne, 2016)[14] is a useful way to identify risk areas, so that they can be corrected. As the importance and prevalence of SmallSat grows, these statistics are needed to inform new reliability processes and standards targeted at these missions. Improved knowledge sharing could be accomplished through an online survey, maybe anonymous to improve response rate.

MODEL BASED APPROACHES

Many of the electronic components developed for traditional large spacecraft do not meet the size and power requirements of SmallSats. By necessity, developers are almost exclusively using electronics produced for the consumer market that are not designed to meet a harsh radiation environment or operate in the temperature range of space. Consequently, no radiation test data exists for these components nor does the manufacturer guarantee the reliability of parts operated outside of the normal operating temperature range. This lack of information is of concern for low earth missions despite the fact that the most harmful and penetrating radiation events are shielded by the earth's magnetic field. However, the environmental hazards are greatly increased in deep space where maintaining normal thermal ranges is more difficult and the ionizing radiation fluxes are higher and more damaging.

The SSRI is evaluating alternatives to the traditional approach to screen and test commercial electronics for two reasons. First and foremost, cost and schedule are typically too constrained to permit a complete radiation and reliability test program for all electronic parts used on a SmallSat. Such test programs can cost millions and easily add years to the schedule. Secondly, the information needed during the design cycle changes.

Moreover, the designer has to have some reasonable confidence the components can survive the mission environment prior to completing the design or risk many redesign cycles as parts fail the environmental tests. This conundrum can be solved through a comprehensive modeling approach that provides some rudimentary insight into the failure modes and component reliability at the onset of a design and matures to predictive part and circuit modeling later in the design cycle.

Inductive Models

The SSRI has identified a number of reliability modeling tools capable of modeling a complex system such a whole spacecraft. The benefit of this class of tools is that the designer can understand risk drivers at the SmallSat level even when the design is at the block diagram level or evaluate the efficacy of design choices such as redundancy. To achieve this level of insight, one might be already well served by using generic reliability information from, for example, multi-junction solar panels flown in the past. While this approach may not capture the true performance of the actual panels, it will be sufficient to evaluate the spacecraft's power distribution system over its lifetime.

The typical structure of such tools is comprised of a functional layer that describes the logical operation of the system and a physical layer that traces faults through a fault tree. In many instances, a statistical layer can be added, where system level failure probabilities and their uncertainties can be computed through a Monte Carlo simulation or through Bayesian Belief Networks. The SSRI is currently evaluating a tool by UCLA[15] to model a notional 6U deep space SmallSat for reliability and radiation effects and build reusable libraries of subsystems that can be adapted by actual SmallSat missions.

The goal is to construct these model libraries to leverage information provided by lower level predictive models (see also next section), or by manufacturers of commercial electronics. Such information sources include data and specification sheets, part macro-models, and process design kits; all of which are readily accessible.

Predictive Models

The second branch of the model-based approach is intended to be predictive.

Of all the environmental effects on microelectronics in space, radiation effects dominate the failure rates. It is safe to say that all digital and mixed signal electronics will experience some level of radiation induced errors and all power electronics will experience a total dose induced performance degradation. The point is that the vast majority of commercial electronics will see either a performance degradation or a non-recoverable failure in the deep space radiation environment.

Still, the space industry has learned to mitigate these radiation effects to a degree at the circuit level (i.e. watchdog timers), the board level (i.e. redundancy) or the system level (i.e. power down during the transit through the South Atlantic Anomaly) as long as the severity and frequency these radiation effects are limited. Therefore, it is imperative to accurately model the radiation effects at the part level, and simulate the impact on the circuit/board as well as the effectiveness of potential mitigation schemes relatively early in the design cycle. One of the challenges is that this requires modeling and simulation approaches that can propagate radiation effects across multiple levels of abstraction from the transistor to the system level.

The SSRI is evaluating a number of radiation-aware modeling tools for the ability to predict radiation effects in various commercial electronic components. The IMPACT tool[16] is an Arizona State University tool to model the total dose effects on bipolar junction transistor (BJT) structures as a function of accumulated dose and dose rate. Initial comparisons with experimental data have demonstrated a good agreement between the code and bipolar components such as regulators, voltage regulators and temperature sensors from various manufacturers.

The next step up in the simulation hierarchy is the Vanderbilt University effort to use the commercial Questa tool by Mentor Graphics[17] to simulate the impact of transistor-level parameter changes arising from total dose irradiation on the system-level behavior of a command and data-handling (C&DH) board for a notional deep space CubeSat. The C&DH board has various analog, digital, mixed-signal, and thermal components that require a diverse set of simulation approaches. Mentor Questa is demonstrated to be a co-simulation platform that can accept models written in SPICE, VHDL, Verilog, and SystemC and simulate them all together with coordinated time stepping. The team constructed radiation models of various components on the C&DH board with parameters that had probability distributions derived from continuous Bayesian regression, Compact model results from the IMPACT tool and radiation test data. Subsequently, a Monte Carlo simulation randomly sampled the parameter distributions in both the radiation and the electrical models. The overall technique was demonstrated on a temperature control loop for the C&DH board. The simulation method predicts an increase of 10 to 15 Kelvin in steady-state temperature, depending on the radiation dose. The same modeling method can be used to predict the impact of radiation on other board-level performance metrics.

THE FUTURE

SSRI is a dynamic initiative, with a goal of improving SmallSat mission confidence in order to facilitate broader use of these platforms for missions where their attributes could enable or enhance objectives or provide other meaningful benefits. The working group will continue to refine a best practices approach to mission confidence. SSRI will also continue to refine a knowledge repository and make it broadly accessible to raise the community's design and development competencies, while continuing to evaluate alternatives to the traditional approach to screen and test commercial electronics. Industry and academia engagement in the effort, contributing their experience, perspectives, and capabilities, will significantly inform its success.

It is vital that metrics are collected to understand how this capability is evolving. CubeSat and SmallSat developers are encouraged to report findings on the CubeSat[18] and SPOON[19] datatbases.

The next TIM will be held in November 2018; these and these and other topics will be discussed and refined at that time.

References

[1] Johnson, M. A., Beauchamp, P., Schone, H., Sheldon, D., Fuhrman, L., Sullivan, E., Fairbanks, T., Moe, M., & Leitner, J (2017). Increasing Small Satellite Reliability – A Public-Private Initiative, *Proceedings of the 31st Annual AIAA/USU Conference on Small Satellites*, Logan, UT, August, 2017, Paper SSC17-WK-03.

[2] Johnson-Roth, G. Mission Assurance Guidelines for A-D Mission Risk Classes, Aerospace Corporation, *TOR-2011(8591)-21*, June 2011.

[3] "Small Satellite Reliability Technical Interchange Meeting (TIM-2) Agenda and Presentations", https://www.nasa.gov/smallsat-institute/reliability-working-group-2.

[4] "Small Satellite Reliability Initiative Technical Interchange Meeting 2 Notes," https://www.nasa.gov/sites/default/files/atoms/files/tim-2_summary_notes.pdf, (October 11-12, 2017).

[5] Royce, W., Managing The Development of Large Software Systems. 1970. http://www-scf.usc.edu/~csci201/lectures/Lecture11/royce1970.pdf.

[6] Incose Systems Engineering Handbook, A Guide For System Life Cycle Processes and Activities.

[7] Encyclopedia of Software Engineering 2nd edition, Johh J. Marciniak, ed., 2001.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Evans, J., Cornford, S., Feather, M.S., "Model Based Mission Assurance (MBMA): NASA's Assurance Future"; Proc. 2016 Reliability and Maintainablility Symposium

[12] Johnson, M.A., et al. (n 1)

[13] Ibid.

[14] Swartwout, M. A. & Jayne, C. University-Class Spacecraft by the Numbers: Success, Failure, Debris. (But Mostly Success.), *Proceedings of the 30th Annual AIAA/USU Conference on Small Satellites*, Logan, UT, August, 2016, Paper SSC-XIII-1.

[15] Groth, K., Wang, C., & Mosleh, A. Hybrid Causal Methodology And Software Platform for Probabilistic Risk Assessment and Safety Monitoring of Socio-Technical Systems. *Reliability Engineering & System Safety*; 95(12), 1276-1285.

[16] Tolleson, B., Adell, P., Rax, B., Barnaby, H., Privat, A., Han, X., Mahmud, A., Livingston, I,. Improved Model for Excess Base Current in Irradiated Lateral PNP Bipolar Junction Transistors, *IEEE TNS* 2018.

[17] "Questa® Advanced Simulator", https://www.mentor.com/products/fv/questa/.

[18] "CubeSat Database", https://sites.google.com/a/slu.edu/swartwout/home/cubesat-database.

[19] "SmallSat Parts On Orbit Now (SPOON)", http://spoonsite.com/.