System Safety & Mission Assurance (SS&MA) for Sub-Class D Missions

TRISMAC
May 2015

System Safety and Mission Assurance Division
Steve Jara Lead Quality Assurance Specialist

Outline:

- NASA Procedural Requirement (NPR) 8705.4 - *Risk Classification for NASA Payloads*
- Why apply SS&MA on Sub-Class D Missions?
- Scoping SS&MA to Sub-Class D Missions
- Challenges of small satellites (e.g. CubeSats)
- Resources and initiatives

NASA's Class D Mission Definition
Reference: NASA Procedural Requirement (NPR) 8705.4 - Risk Classification for NASA Payloads

NASA's Class D Mission Definition

Reference: NASA Procedural Requirement (NPR) 8705.4 - *Risk Classification for NASA Payloads*

Characterization	Class D
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	Low priority, high risk
National Significance	Low to medium
Complexity	Medium to low
Mission Lifetime (Primary Baseline Mission)	Short < 2 years
Cost	Low
Launch Constraints	Few to none
In-Flight Maintenance	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	Medium or significant risk of not achieving mission success is permitted. ***Minimal assurance standards are permitted.***

Sub-Class D Missions: Low budget, fast paced projects (~$50M, 2 years) executed under a set of streamlined processes aimed at mitigating only the most significant risks to mission success. They are normally executed by/with:

- An atmosphere of innovation & creativity
- Cross-trained thinly spread teams (with limited oversight)
- A high percentage of COTS & low heritage parts
- A high degree of reliance on vendor SS&MA processes
- An open-loop “make-it-work” corrective action system
- An emphasis on cost & schedule

Why apply SS&MA on Sub-Class D Missions?

- **Traditional arguments against:**
  - Stifles innovation & creativity (rules based)
  - Too costly & time consuming
  - Unnecessary when risk of mission failure is acceptable
- **The real story; SS&MA is critical to mission success:**
  - Tailorable, flexible, & identifies where rules are good enough or where innovation is required
  - Cost can be limited to initial risk assessments followed by the mitigation of the most significant risks
  - Ensures projects allocate their limited resources judiciously and intelligently

Mission failure is not acceptable due to blindly/poorly applied processes; SS&MA provides critical insight & intelligence

The Clash between Traditional SS&MA & Sub-Class D Mission Characteristics

Traditional SS&MA	Sub-Class D Missions
A conservative (risk-adverse) approach & a rigorous adherence to a comprehensive set of established rules	An atmosphere of innovation & creativity complimented by an agile & surgical application of tailored requirements/guidelines
Performed by independent SS&MA specialists (not responsible for the project's cost/schedule)	Executed by cross-trained thinly spread teams (with limited oversight)
A high degree of independent verification & validation (V&V) as applied to the assembly, subsystem, & system levels	A limited degree of V&V usually performed at the system level (which includes a high percentage of COTS & low heritage parts)
An extensive document library, wordy plans for each SS&MA element (Safety, QA, CM, Risk Management, Orbital Debris Assessments, etc.), & a flow down of process requirements throughout the supply chain	A minimal set of documents with several disciplines combined into one plan & a high degree of reliance on vendor SS&MA processes
A closed-loop root cause analysis based corrective action system	An open-loop "make-it-work" corrective action system
A de-emphasis on its impact to project cost & schedule	An emphasis on cost & schedule

Scoping SS&MA to Sub-Class D Missions (Summary)

Traditional SS&MA	Sub-Class D Missions Characteristics	Optimizing the amount of SS&MA for Sub-Class D Missions (Depends on empowering & guiding all project personnel on how to integrate SS&MA into their work & providing them SS&MA specialist when needed)

A conservative (risk-adverse) approach & a rigorous adherence to a comprehensive set of established rules	An atmosphere of innovation & creativity complimented by an agile & surgical application of tailored requirements/guidelines	• Ensure appropriate level of QA is chosen and agreed to by all stakeholders
		  o Don't overlay AS9100 or ISO9001 when test & inspection requirements are sufficient
		• Prioritize the order in & degree to which SS&MA actions are implemented based on:
		  o Project risk , phase, schedule, & budget (as assessed based on the content of the project plan & concept of operations)
		• Use peer reviews/assessments to optimize the level of SS&MA

Performed by independent SS&MA specialists (not responsible for the project's cost/schedule)	Executed by cross-trained thinly spread teams (with limited oversight)	• Embed/integrate SS&MA into all project elements & phases
		  o Cross-train key project personnel in basic SS&MA principles
		  o Hold everyone responsible for SS&MA, but name one person as the SS&MA lead
		  o Ensure SS&MA is a topic during all project meetings & reviews
		  o Use peer reviews to compensate for the lack of independence

A high degree of independent verification & validation (V&V) as applied to the assembly, subsystem, & system levels	A limited degree of V&V usually performed at the system level (which includes a high percentage of COTS & low heritage parts)	• Identify critical SS&MA requirements & their flow down considering critical:
		  o Mission operations, systems, designs, & acquisitions
		  o Manufacturing, testing, & operations activities
		  o Historical issues, best practices, & lessons learned
		• Witness only those tests (including the test set-up) that are deemed to be the highest risk

An extensive document library, wordy plans for each SS&MA element, & a flow down of process requirements throughout the supply chain	A minimal set of documents with several disciplines combined into one plan & a high degree of reliance on vendor SS&MA process	• Streamline/reduce documentation & identify critical SS&MA clauses to include in specifications & contracts
		• Establish & make use of prescreened vendors
		  o Augment with vendor site visits and/or
		  o Bench audits of vendor procedures

A closed-loop root cause analysis based corrective action system	An open-loop "make-it-work" corrective action system	• Limit root cause analysis to:
		  o Safety critical issues
		  o Negative trends & repeat issues
		  o Out-of-family results

A de-emphasis on its impact to project cost & schedule	An emphasis on cost & schedule	• Baseline the SS&MA plan off of a detailed concept of operations • Limit SS&MA to safety critical & first flight items & the most significant risks to mission success • Limit external/specialized SS&MA support

Small Spacecraft SMA Challenges

Small Spacecraft SMA Challenges

- **Small spacecraft projects usually have the following features:**
  - Standardized interfaces (i.e. EELV Secondary Payload Adapter (ESPA) (rings), standard form (cubesats) and containerization (i.e. P-PODS) for rideshare launches
  - "Build and test" versus extensive analysis of design
  - Greater use of commercial off-the-shelf parts
  - Lower cost
  - Rapid development
  - Higher risk tolerance
  - Lower barrier-to-entry for space missions (university and small business researchers, etc.)
  - Possibility for unique applications
- **These features pose potential safety and mission assurance challenges and risks.**
- **Deployment of small satellites that are too small to be detected by the Space Surveillance Network also poses a potential collision risk to other spacecraft.**
- **Deployment of large constellations of small satellites could potentially worsen the orbital debris problem.**

Definition of Small Spacecraft @NASA:

"Small" is defined as less than 180 kg –based on the maximum mass for an ESPA-class secondary satellite payload.

To be considered a "spacecraft" it must separate from its launch vehicle and operate independently for at least some portion of its mission in space. In additional to satellites and probes, small entry vehicles and landing craft can be small spacecraft. Spacecraft deployed from and/or operating independently around the ISS or other space system can be small spacecraft.

Typically small spacecraft are launched as secondary payloads, although small launch vehicles could deliver small spacecraft as primary payloads.

Sounding rocket payloads and attached or hosted payloads that remain attached to their host spacecraft or launch vehicle throughout their operational mission are not considered small spacecraft.

We do not consider balloon payloads to be small spacecraft.

Additional Definitions:
Minisatellite: 100 kg or higher
Microsatellite: 10-100 kg
Nanosatellite: 1-10 kg
Picosatellite: 0.01-1 kg
Femtosatellite: 0.001-0.01 kg

A cubesat is a special category of nanosatellite. One cubesat unit (1U) has dimensions of 10 by 10 by 11 centimeters. Cubesats have been built in 1U, 1.5U, 2U, 3U and 6U sizes.

Small Spacecraft Community of Practice

- To help support small spacecraft development, OSMA initiated a Small Spacecraft Community of Practice (CoP) on the NASA Engineering Network (NEN) in December 2013 and co-leads this CoP along with the Small Spacecraft Technology Program Executive in Space Technology Mission Directorates.

- The CoP serves as forum for representatives from NASA Flight Projects, Engineering, Safety and Mission Assurance, Science, Space Technology, and Human Exploration and Operations Directorates to share challenges, approaches, and lessons learned for development of small spacecraft projects, including the implementation of safety, mission assurance, design, and test guidelines and requirements.

Small Spacecraft CoP (continued)

- Subtopics established in the CoP include the following Safety and Mission Assurance disciplines: Workmanship, Software Assurance, Reliability, Quality Assurance, EEE Parts, Orbital Debris Mitigation and Meteoroid Environment. Applicable guidance documents and links to other resources; websites, including OSMA and ODPO websites; and "ask the experts" point of contacts (POCs) are provided on the CoP.

- Membership of the small spacecraft CoP is 100+ with members from the NASA Centers and HQ. Access to the information of small spacecraft CoP is limited to NASA badged personnel. Future plans are to post the guidance that S&MA develops for high-risk tolerant/small spacecrafts to the OSMA website for public access.

- A Risk Class D/CubeSat EEE Parts tiger team has been initiated to develop guidance for EEE parts selection for small spacecraft

Other Resources and Initiatives

- LSP-REQ-317.01, Launch Services Program Level Dispenser and CubeSat Requirements Document defines the Launch Services Program (LSP) program level and technical requirements placed on containerized CubeSat dispenser and Picosatellite (CubeSats) satellites for integration on NASA LSP ELV mission. This document is available of the small spacecraft CoP.
- LSP is also developing a “CubeSat 101” guidance document and plans to complete this document later this year.
- The NASA Orbital Debris Program Office initiated a study last year to assess the impact of Cubesat deployment on the orbital debris environment. The study is expected to be completed in September 2015. In addition, plans are to update the NASA Standard 8719.14 to provide requirements on Cubesat design and deployment (e.g, configured so that they are trackable).