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

NEPP
June 24, 2015

System Safety and Mission Assurance Division
Steve Jara

Outline:

- NASA Procedural Requirement (NPR) 8705.4 - *Risk Classification for NASA Payloads*
- ARC's Class D Philosophy
- Why apply SS&MA on Sub-Class D Missions?
- Risk Based Approach with SS&MA
- Scoping SS&MA to Sub-Class D Missions
- Small Spacecraft Community of Practice

National Aeronautics and Space Administration

Ames
Discovery Innovations Solutions

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.***

ARC's Class D Philosophy

- ARC complies with the NPR 8705.4 requirements for Class D missions
  - **Minimal assurance standards are permitted:** ***except where safety would be compromised***
- ARC projects define their minimal assurance standards based on documents developed by the engineering and SS&MA Technical Authorities (TAs) including:
  - Ames Procedural Requirements (APR) 8070.2 - *Class D Spacecraft Design and Environmental Test* document
  - APR 8730.2 - *Electrical, Electronic, and Electromechanical (EEE) Parts Control Requirements*
  - APR 7150.2 – *NASA Ames Research Center Software Engineering Requirements*
  - APR 8705.1 - *System Safety and Mission Assurance*
- Note: The ARC SS&MA Division is drafting an APR for Class D specific SS&MA
  - APR 8705.2 - *System Safety and Mission Assurance for Class D Missions*

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

Risk-Based Approach with SS&MA

- **Class D Missions are not risk free and can have Class A, B, or C elements which means the Project will have numerous risks requiring mitigation**
  - Hazard identification and risk assessments are critical to ensuring SS&MA resources are applied optimally
  - These identifications and assessments must start early in the project's formulation phase and include SS&MA
- **Risks change over the project's life cycle and must be continuously managed to ensure they do not exceed the acceptable risk threshold**
- **This integrated and continuous process allows the project, SS&MA, and stakeholders to have an "Eyes Wide Open" view as they move forward through the life cycle and ensures the:**
  - Optimum use of SS&MA resources
  - Intelligent use of project funding reserves

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 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.

Conclusions

- **Each Class D project varies in cost, mission length, schedule, and:**
  - Operational environment, critical systems, complexity, operations, etc.
- **All these areas must be assessed as the project balances its level of risk with its mission success criteria**
- **Integrating SS&MA early into the project ensures all requirements are properly defined and that SS&MA specific tasks are scoped within the project's established risk posture**
- **There are many credible SS&MA requirement reductions for Class D missions that will help control and reduce their cost including:**
  - Streamlined processes for CM, PRACA, and I&T travelers
  - Transitioning to an insight rather than oversight level of SS&MA for COTS, preapproved suppliers, and other low risk tasks
  - Intelligently applying a risk-based approach to determine where to apply SS&MA resources