Scalable mission assurance and a construct for increasing mission tempo

SmallSat Conference August 2018

Dr. David Voss - AFRL (Presenter)

Dr. Lee Jasper, Mr. Paul Oppenheimer – SDL

Dr. Lauren Hunt, Ms. Charlene Jacka – AFRL
Large Strategic Investments

- Large infrastructure
- Large dollar investments
- Fully owned by the Government or commercial companies
- Long timelines
- Space is different/harder/special

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This approach is proposed and has not been approved by the Air Force.
How We Should Think Of Space

- We should view satellites as part of a network
  - Satellites may be trunk lines
  - They may be significant nodes
  - They may be minor nodes
- Every domain has its own challenges
- Every problem/challenge should pull from as many domains as possible
- Space should represent all players
- We should understand the confidence from each source

The Internet network: nodes are computers or post-pc devices and links are wired or wireless connections between them
The Need for Higher Throughput

How we Currently Think of Space

- Large infrastructure
- Large dollar investments
- Fully owned by the Government
- Long timelines
- Space is different/harder/special
- SPOs own satellite programs not missions

How We Should Think Of Space

- We should view satellites as part of a network
  - Satellites may be trunk lines
  - They may be significant nodes
  - They may be minor nodes
- Every domain has its own challenges
- Every problem/challenge should pull from as many domains as possible
- Space should represent all players
- We should understand the confidence from each source

How do we get from here to there?
WHY DOES MISSION ASSURANCE EXIST?

Log Cost

Mission Assurance

100%

50%

Optimal for rapid prototyping

Not good value

Typical Larger Satellite Programs

$ $ $$

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This approach is proposed and has not been approved by the Air Force.
Mission scope fits into capabilities and complexity available given technical, programmatic and oversight needs.

Mission scope is static and resources applied to achieve that mission.

Build your own box.
1. Constraint-driven missions are the most common

2. Class D mission assurance practices are significantly modified or ignored

3. Class D overhead can dilute the full potential contribution of small satellites

FASTER INNOVATION | LOW-COST DEVELOPMENT | EDUCATIONAL OPPORTUNITIES
What are the minimum practices I should use to meet constraint-driven goals?

How can I push the boundary of faster innovation while still achieving an acceptable Return-on-Investment?
At inception, the stakeholders and designers should have an honest conversation about whether the mission is requirements or constraint driven.
## Technical Implementation Taxonomy

<table>
<thead>
<tr>
<th>Class</th>
<th>Example Technical Activities</th>
<th>Programmatic</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td><strong>Extremely Critical, Operational</strong> - Missions are extremely critical operational systems where all practical measures are taken to ensure mission success. They have the highest cost, are of high complexity, and the longest mission life with tight launch constraints.</td>
<td>Fully requirement driven; cost/schedule allow confirmation of full mission success with absolute minimal residual risks</td>
</tr>
<tr>
<td>B</td>
<td><strong>Critical, Operational or Demo Op</strong> – Missions are defined as critical operational, exploration, and technical demonstrators in which only minor compromises are taken in stringent processes for mission success to achieve a low risk profile. The criteria for minor compromises include allowing controlled single point failures, proto-flight hardware, Level/Grade 2 EEE parts, reduced circuit analysis, etc.</td>
<td>Fully requirement driven; cost/schedule allow confirmation of full mission success with few residual risks</td>
</tr>
<tr>
<td>C</td>
<td><strong>Less Critical, Exploratory or Experimental</strong> – Missions are defined as lower national significance, exploratory or experimental missions, with a reduced set of MA standards applied resulting in a moderate risk profile.</td>
<td>Fully requirement driven; cost/schedule allow confirmation of full mission success with moderate residual risks</td>
</tr>
</tbody>
</table>
| D     | **Experimental (Full Requirements Driven)** - All of the below, plus:  
  • Full functional and performance testing  
  • Worst Case Analyses & design  
  • NPR 8705.4, TOR-2011(8591)-21 | Fully requirement driven; cost/schedule allow confirmation of full mission success but with higher residual risks |
| E     | **Full (Constrained) Mission Success** - All of the below, plus:  
  • Environmental characterization and flow into requirements (i.e. radiation)  
  • Full functional and limited performance testing  
  • More detailed FTA & FMEA (flight, ground, GSE), SPF analysis/redundancy  
  • Requirement development to at least L2 and V&V | Less capability constrained and more requirement driven; cost/schedule allow confirmation of capability to achieve full mission success |
| F     | **Minimum Mission Success** – Add full command testing, DITL, common mission-modes, items to address mission-specific risks, thermal analysis | Mostly capability constrained; cost/schedule allow confirmation of capability to achieve minimum mission success |
| G     | **Survival** – Add critical survival testing (power, comm. for tumble cases, charge/discharge, TVAC) | Mostly capability constrained; cost/schedule doesn’t allow significant confirmation of capability beyond survival |
| H     | **Do no harm** – Range safety, do-no-harm environments, de-orbit compliance | Fully capability constrained; bare minimum cost/schedule |
### Technical implementation taxonomy

<table>
<thead>
<tr>
<th>Demonstrated Level of Capability</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do No Harm</td>
<td>DOA is ok (education and/or fully constrained and not requirement driven)</td>
</tr>
</tbody>
</table>

All missions are designed for full mission success; the amount of mission assurance can provide a level of confidence in mission success.
<table>
<thead>
<tr>
<th>Demonstrated Level of Capability</th>
<th>Example Technical Activities</th>
<th>Example Approval Authority (AA)/Oversight</th>
<th>Programmatic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do No Harm</td>
<td>Vibration testing, bake out, inhibit design review/test, range safety measures demonstrated, no RF transmission within 45 minutes of deployment/no attitude maneuvers within 15 minutes, 25 year deorbit.</td>
<td>AA: Program Reviews: informal peer, launch readiness.</td>
<td>Fully constrained, schedule + cost allow launch requirement verification only</td>
</tr>
<tr>
<td>Survival</td>
<td>(All of the above), possibly designing power/comm for tumble, long range communications testing with ground station has been completed(1), complete charge/discharge cycle testing completed(2), TVAC.</td>
<td>AA: Program Reviews: informal peer, may have stakeholder.</td>
<td>Mostly constrained, schedule + cost do not allow significant confirmation of capability beyond survival</td>
</tr>
<tr>
<td>Minimum Functionality</td>
<td>(All of the above), full command execution test(3), startup/POR DitL testing(4), Sun-point test(5), other mission specific tests demonstrating survival functionality, mission specific FTA &amp; Self-EMC test, thermal analysis.</td>
<td>AA: Program +1 level Stakeholder input Reviews: informal-SCR, PDR, CDR, TRR, LRR</td>
<td>Mostly constrained, schedule + cost allow confirmation of capability to achieve minimum success</td>
</tr>
<tr>
<td>Nominal (constraints)</td>
<td>(All of the above), environmental characterization and flow down into requirements (i.e. radiation), full functional and limited performance testing, more detailed FTA &amp; FMEA (flight, ground, GSE), SPF analysis/redundancy, requirement development to at least L2 and V&amp;V.</td>
<td>AA: Program +2 levels Stakeholder input/vote Reviews: formal-SCR, PDR, CDR, TRR, LRR.</td>
<td>Less constrained and more requirement driven, schedule + cost allow confirmation of capability to achieve full success</td>
</tr>
<tr>
<td>Nominal (requirements)</td>
<td>(All of the above), full functional and performance testing, Worst Case Analyses &amp; design. NPR 8705.4, TOR-2011(8591)-21</td>
<td>AA: Director Stakeholder vote/driven</td>
<td>Fully requirement driven, schedule + cost allow confirmation of capability to achieve full success</td>
</tr>
</tbody>
</table>
**Programmatic Implementation Example**

**Programmatic Cat 3 Missions**
- Historical Class A-D
- Above a certain Max $ value
- Well Understood

**Programmatic Cat 2 Missions**
- Embraces New Space parts and practices
- Above a certain moderate $ value
- Medium Risk

**Programmatic 1 Missions**
- Embrace terrestrial systems embedded systems practices
- Most affordable $ value
- High Risk

<table>
<thead>
<tr>
<th>Class</th>
<th>Example Technical Activities</th>
<th>Programmatic</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Extremely Critical, Operational - Missions are extremely critical operational systems where all practical measures are taken to ensure mission success. They have the highest cost, are of high complexity, and the longest mission life with tight launch constraints.</td>
<td>Fully requirement driven; cost/schedule allow confirmation of full mission success with absolute minimal residual risks</td>
</tr>
<tr>
<td>B</td>
<td>Critical, Operational or Demo Op - Missions are defined as critical operational, exploration, and technical demonstrators in which only minor compromises are taken in stringent processes for mission success to achieve a low risk profile. The criteria for minor compromises include allowing controlled single point failures, proto-flight hardware, Level/Grade 2 EEE parts, reduced circuit analysis, etc.</td>
<td>Fully requirement driven; cost/schedule allow confirmation of full mission success with few residual risks</td>
</tr>
<tr>
<td>C</td>
<td>Less Critical, Exploratory or Experimental - Missions are defined as lower national significance, exploratory or experimental missions, with a reduced set of MA standards applied resulting in a moderate risk profile.</td>
<td>Fully requirement driven; cost/schedule allow confirmation of full mission success with moderate residual risks</td>
</tr>
<tr>
<td>D</td>
<td>Experimental (Full Requirements Driven) - All of the below, plus: • Full functional and performance testing • Worst Case Analyses &amp; design • NPR 8705.4, TCR-2011(8559)-21</td>
<td>Fully requirement driven; cost/schedule allow confirmation of full mission success but with higher residual risks</td>
</tr>
<tr>
<td>E</td>
<td>Full (Constrained) Mission Success - All of the below, plus: • Environmental characterization and flow into requirements (i.e. radiation) • Full functional and limited performance testing • More detailed FTA &amp; EMEA (flight, ground, GSE), SPF analysis/redundancy • Requirement development to at least L2 and V&amp;V</td>
<td>Less capability constrained and more requirement driven; cost/schedule allow confirmation of capability to achieve full mission success</td>
</tr>
<tr>
<td>F</td>
<td>Minimum Mission Success - Add full command testing, DIIT, common mission-modes, items to address mission-specific risks, thermal analysis</td>
<td>Mostly capability constrained; cost/schedule allow confirmation of capability to achieve minimum mission success</td>
</tr>
<tr>
<td>G</td>
<td>Survival – Add critical survival testing (power, comm. for tumble cases, charge/discharge, TVAC)</td>
<td>Mostly capability constrained; cost/schedule doesn’t allow significant confirmation of capability beyond survival</td>
</tr>
<tr>
<td>H</td>
<td>Do no harm – Range safety, do-no-harm environments, do-orbit compliance</td>
<td>Fully capability constrained; bare minimum cost/schedule</td>
</tr>
</tbody>
</table>

9 August 2018

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This approach is proposed and has not been approved by the Air Force.
Conclusions

• New mission assurance profiles are needed that represent constraint driven mission sets

• Oftentimes we trade science and technology requirements for schedule or cost savings

• A clear scope and broad understanding of constraints drive implemented MA to have the greatest ROI

• Generally more constrained missions allow decisions in all areas to be made closer to the project implementers (drive decision authority as low as possible)

Is this the right path? We want to engage with the community!
Case study: Competing objectives/constraints

SCENARIO: Multi-organization teaming

University Desired Approach: SURVIVAL

Professor believes educational intent met if some communication with satellite is achieved

→ Work must primarily be done by students (mostly new team, 2nd sat of university)
→ Having the same students go through the entire process provides the best educational experience (~80% turnover in 2 years)
→ Need additional program funding

Company X Desired Approach: FULL SUCCESS

Company X wants to show their product works as expected on-orbit

→ Only has internal funding to support spacecraft development activities related to their payload
→ No flight heritage of this product, paying customers not ready to assume risk
→ Product is batch produced and as a result, several flight models are available

Launch Provider Y Expectation: DO NO HARM

Launch Provider Y is primarily concerned with safety of their launch vehicle on its first flight

→ Schedule is 100% driven by the launch provider since they are financing this first flight.
→ Safety to the flight vehicle is non-negotiable

MISSION ASSURANCE RESULT: SURVIVAL

Team/Stakeholder Discussion:
• University/Company X need teaming opportunities to achieve goals, both benefit from launch provider involvement
• Time is key driver- launch provider will not provide schedule flexibility & value to individual students decreases as development extends beyond their academic term
• Knowing that inexperienced personnel would be performing most of the spacecraft development work, Company X recognized it could mitigate some risk by flying with several university teams who have programs operating on similar timelines

9 August 2018

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This approach is proposed and has not been approved by the Air Force.
Case study: Competing objectives/constraints

SCENARIO: Multi-organization teaming

University Desired Approach: SURVIVAL
- Professor believes educational intent met if some communication with satellite is achieved
- Work must primarily be done by students (mostly new team, 2nd sat of university)
- Having the same students go through the entire process provides the best educational experience (~80% turnover in 2 years)
- Need additional program funding

Company X Desired Approach: FULL SUCCESS
- Company X wants to show their product works as expected on-orbit
- Only has internal funding to support spacecraft development activities related to their payload
- No flight heritage of this product, paying customers not ready to assume risk
- Product is batch produced and as a result, several flight models are available

Launch Provider Y Expectation: DO NO HARM
- Launch Provider Y is primarily concerned with safety of their launch vehicle on its first flight
- Schedule is 100% driven by the launch provider since they are financing this first flight.
- Safety to the flight vehicle is non-negotiable

MISSION ASSURANCE RESULT: SURVIVAL
Practical Implementation:
- All Do no harm/Survival testing
- DitL testing and full command execution test only if time permits
- Internal university reviews and approval, Company X supports all, but does not pass/fail, launch provider attends from CDR on, has final say in LRR
Case Study: Multi-Level Mission Assurance

Scenario: Company X plans to field a constellation of satellites

Phase 1: One satellite for proof-of-concept demo, use lessons learned in Phase 2
Phase 2: Field full constellation
Key Driver: Time – want to be first to market, investor ROI

Discussion

Investors & developers agree imperfect functionality in Phase 1 demo is acceptable as long as path forward exists by Phase 2
Testing the full set of satellites may be time intensive, especially if high-confidence in performance is needed before launch

Mission Assurance Result:
MIXED
Phase 1: SURVIVAL
- Company X chooses lower MA approach to realize near-term results and maintain momentum
Phase 2: NOMINAL for a few/ MINIMUM SUCCESS for most
- One vehicle per batch undergoes rigorous testing for systematic failures, remainder undergo minimal assurance
- Phasing of production & launch staggered to allow improvements; (i.e. Full Mission Success assurance through on-orbit testing/demo instead of purely ground assurance practices

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This approach is proposed and has not been approved by the Air Force.