Terminology: High Confidence

• You want a system and execution approach that generates *HIGH CONFIDENCE* when:
  – It’s a single vehicle that *has got to work* (no opportunity to refly)
  – It’s a multi-vehicle system that needs *every vehicle to work* (no vehicle redundancy, no opportunity for a second launch)

• You can achieve *HIGH CONFIDENCE* through various combinations of:
  – Part, component, and vehicle redundancy
  – EEE parts selection
  – Design practices and margins
  – Previous flight and system experience; heritage
  – Testing (HW and SW) and requirements verification
  – Spares policy
  – Design iterations (e.g. breadboards, EMs, Qual units, flight units)
• You could say you have a system and execution approach in which there may be *LOW CONFIDENCE* when:
  – It’s a completely new item (system, component, application, environment….) (aka low TRL)
  – It hasn’t been analyzed or tested
  – Operational environment is unknown (e.g. launch vibe, radiation) or unproven (e.g. first flight of launch vehicle)

• Proceeding with a *LOW CONFIDENCE* approach or component can be okay when:
  – It’s a demo or prototype
  – It’s “inexpensive” and another can be made
  – Reflight is readily available (fly-fail-fix-fly again)
  – Time scales are “fast”
Recommendations

• Reliability Subcommittee should:
  – Capture characteristics of missions / systems for which $HIGH$ CONFIDENCE is expected
  – Capture characteristics of missions/systems for which $LOW$ or $MEDIUM$ CONFIDENCE is acceptable
  – Outline priorities for increasing the confidence level of a component, system, or approach

• Proposed output (Guideline Document):
  – Decision criteria for when to use Guidelines as opposed to NASA and other Standards (7120, INST-002…)
    • Some missions, especially NASA deep space, may use CubeSats / SmallSats but effectively still be “Class D” or above (?)
  – Focus on $RAPID$ $SPACE$
    • Fast, cheap, “failure is acceptable” missions
Example
### Mission Characteristics

<table>
<thead>
<tr>
<th>Classification → Mission Type ↓</th>
<th>High Confidence Required when</th>
<th>Moderate Confidence Acceptable when</th>
<th>Low Confidence Acceptable when</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep space</td>
<td>5-10 years operation expected</td>
<td>1-3 years</td>
<td>Up to months</td>
<td></td>
</tr>
<tr>
<td>LEO</td>
<td>5+ years operation expected</td>
<td>~ 1 year</td>
<td>Months</td>
<td></td>
</tr>
<tr>
<td>Mission Criticality</td>
<td>Operational mission; national security</td>
<td>Experimental; tech demo; tech maturation</td>
<td>Tech demo; teaching</td>
<td></td>
</tr>
<tr>
<td>Reflight</td>
<td>First launch has to work (no reflight possible)</td>
<td>Rapid reflight available</td>
<td>OK to try again on another launch opportunity</td>
<td></td>
</tr>
<tr>
<td>Repeat cost</td>
<td>Build / launch / operate another is too expensive</td>
<td></td>
<td>Fix / design / build a new one costs are low</td>
<td></td>
</tr>
<tr>
<td>Operational Criticality</td>
<td>Single vehicle / every vehicle has got to work</td>
<td>“Down time” is acceptable</td>
<td>System as a whole is resilient to individual failures</td>
<td></td>
</tr>
</tbody>
</table>
## Reviews #1

<table>
<thead>
<tr>
<th>Classification → Reviews↓</th>
<th>When High Confidence is needed</th>
<th>When Moderate Confidence is expected</th>
<th>When Low Confidence is acceptable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRR, MCR, SDR, MDR (Combine into a single “Mission / System Design Review” – M/SDR)</td>
<td>Add mission radiation effects analysis to discussion.</td>
<td>Add mission radiation effects analysis to discussion.</td>
<td>Focus on driving requirements, mass and power margins</td>
<td>For all confidence levels: Are the requirements: Complete - Address objectives and needs of sponsor What is missing/ What are driving requirements?</td>
</tr>
<tr>
<td></td>
<td>“Large” SRB (1-2 sponsor reps, 1-2 system engineers, 1 each engineer with expertise in the areas of the driving requirements, mission objectives / science, I&amp;T).</td>
<td>Medium SRB (1 sponsor rep, 1-2 system engineers, 1 each engineer with expertise in the areas of the driving requirements and of mission objectives / science)</td>
<td>Small informal SRB (1 sponsor rep, 1-2 system engineers, 1 engineer with expertise in the area of the driving requirements).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Design: address what commercial items will be bought and what items will be custom design. Discuss heritage and approach for commercial items. Discuss heritage and approach for custom items and how they interface to commercial items. Discuss integration approach.</td>
<td>System Design: address what commercial items will be bought and what items will be custom design; focus on custom items and how they interface to commercial items.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Development team conducts internal peer review of requirements prior to M/SDR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Development Units and Spares - #1

<table>
<thead>
<tr>
<th>Classification → Item ↓</th>
<th>When High Confidence is needed</th>
<th>When Moderate Confidence is expected</th>
<th>When Low Confidence is acceptable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering Models</td>
<td>Recommended for payload and spacecraft bus</td>
<td>Not typically included</td>
<td>Not typically included</td>
<td>EMs / EDUs are always a good idea if you can afford the cost and schedule</td>
</tr>
<tr>
<td>Flight spare components</td>
<td>Sparing at component level for payload and critical items</td>
<td>Sparing at component level for payload and critical items</td>
<td>Not typically included</td>
<td></td>
</tr>
<tr>
<td>I&amp;T of spares, EMs, EDUs</td>
<td>For large “flocks”, might build and test a full spare vehicle.</td>
<td>Often used for early interface testing, fit checks, and procedure development</td>
<td>Usually only if /when primary unit(s) have problems</td>
<td>Can also test all units and cherry pick best-performing item for flight</td>
</tr>
<tr>
<td>Qual unit</td>
<td>Recommended</td>
<td>Not typically included</td>
<td>Not typically included</td>
<td></td>
</tr>
<tr>
<td>Vendor testing of procured components</td>
<td>Vendor has done qual level testing of design, acceptance testing of delivered items</td>
<td>Vendor has done qual level testing of design preferred</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
# Design Management

<table>
<thead>
<tr>
<th>Classification → Design Activity ↓</th>
<th>When High Confidence is needed</th>
<th>When Moderate Confidence is expected</th>
<th>When Low Confidence is acceptable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanical drawings</td>
<td>Review and signature(s) for critical parts</td>
<td>Review at discretion of team</td>
<td>Sketches of custom parts if needed; peer review at discretion of team</td>
<td></td>
</tr>
<tr>
<td>CAD Model</td>
<td>CAD model to box level, including cabling, stowed and deployed configurations</td>
<td>Representative CAD model useful for I&amp;T and estimation of mass properties; stowed and deployed configurations</td>
<td>Representative CAD model useful for I&amp;T and estimation of mass properties; stowed configuration at a minimum</td>
<td>Generally at board level and above</td>
</tr>
<tr>
<td>Configuration Control</td>
<td>Configuration control of custom mechanical parts drawings; FSW</td>
<td></td>
<td>Developer version control of sketches and FSW</td>
<td></td>
</tr>
</tbody>
</table>
## Abbreviations, Acronyms, Initialisms

- **CAD** = Computer-Aided Design
- **CADRe** = Cost Analysis Data Requirement
- **CDR** = Critical Design Review
- **DDT&E** = Design, Development, Test and Evaluation
- **DOD** = Department of Defense
- **DoD** = Depth of Discharge
- **EDU** = Engineering Development Unit
- **EM** = Engineering Model
- **EMC** = Electromagnetic Compatibility
- **EMI** = Electromagnetic Interference
- **EOM** = End of Mission
- **ESP** =
- **EVM** = Earned Value Management
- **FMEA** = Failure Modes and Effects Analysis
- **FRR** = Flight Readiness Review
- **FSW** = Flight Software
- **GEO** = Geosynchronous, Geostationary
- **GIDE** =
- **GTO** = GEO Transfer Orbit
- **HDP** = Hardware Development Plan
- **IMS** = Integrated Master Schedule
- **I&T** = Integration and Test
- **KDP** = Key Decision Point
- **LCC** = Life-cycle Cost estimate
- **LEO** = Low Earth Orbit
- **MAP** = Mission Assurance Plan
- **MCR** = Mission Concept Review
- **MDR** = Mission Definition Review
- **MRB** = Materials Review Board
- **MRR** = Mission Readiness Review
- **NASA** = National Aeronautics and Space Administration
- **ORR** = Operational Readiness Review
- **PDR** = Preliminary Design Review
- **PER** = Pre-Environmental (Test) Review
- **PSR** = Pre-Ship Review
- **R&D** = Research and Development
- **RFA** = Request for Action
- **RID** = Review Item Discrepancy
- **RMP** = Risk Management Plan
- **SDP** = Software Development Plan
- **SDR** = System Definition Review
- **SEMP** = Systems Engineering Management Plan
- **SRB** = System Review Board
- **SRR** = System Requirements Review
- **TRR** = Test Readiness Review
- **TVAC** = Thermal-Vacuum (test)
- **WBS** = Work Breakdown Structure
Contact Information for Feedback

Miquel Moe
NASA GSFC
Miquel.a.moe@nasa.gov
(301) 286-2281

Linda Robeck Fuhrman
MIT-Lincoln Laboratory
Linda.fuhrman@ll.mit.edu
(781) 981-4949