Safe and reliable, all the way to Mars and back:
The role of the International Space Station in developing, and verifying safe, reliable human interplanetary transport

Steve Koontz\textsuperscript{1}, Patrick O’Neill\textsuperscript{1}, Brandon Reddell\textsuperscript{1}, Thomas Keeping\textsuperscript{1}, Kristina Rojdev\textsuperscript{1}, Joseph Minow\textsuperscript{2}, William Atwell\textsuperscript{3} and Paul Boeder\textsuperscript{3}

\textsuperscript{1}NASA Johnson Space Center, Houston, TX 77059 USA, \textsuperscript{2}NASA Marshall Space Center, Huntsville, AL 35812
\textsuperscript{3}Boeing Research & Technology, Houston, TX 77059 USA
The character of long-term (1-3 years) human interplanetary space flight will lead to safety and reliability requirements more demanding (and costly) than any previously encountered. Remember, if it isn’t reliable it isn’t safe.

- To date, spacecraft crews have never been more than a few hours-to-days away from a safe emergency landing.
- There are no comparable quick/safe Earth return options for the crew of an interplanetary transport a few months out from Earth. In that case, failure really isn’t an option.
- Spacecraft electronics (avionics) systems reliability (and crew safety) depends on:
  - Generic hardware/software quality and durability in the space flight environment
  - Component/system sensitivity to the space radiation environments, especially the total ionizing dose (TID) and Single Event Effects (SEE) environments

The primary focus of this paper is spacecraft avionics reliability in the SEE environment.
The Single Event Effects (SEE) environment and its effect on spacecraft avionics systems

- Space flight ionizing radiation (IR) environments are radically different from the IR environments we are exposed to on Earth
  - Highly energetic charged particles (atomic nuclei and electrons) dominate the space flight environment
    - Galactic cosmic “rays”, trapped protons, and solar particle event (SPE) charged particles
    - Much smaller contributions from x-rays and gamma rays which contribute to TID only
- High energy charged particles cause SEE in spacecraft avionics components
  - Energetic charged particles produce transient high density ionization tracks when passing through matter
  - High density ionization tracks cause SEE in solid state electronic devices
    - Soft errors that are correctable, e.g. single event upsets for bit flips in digital memory
    - Hard device failures that fail the equipment, e.g. single event gate rupture or burn-out

Primary and secondary cosmic ray ionization tracks through the depletion region (white) of the PN junction (P light grey; N dark grey) in a solid state device enables transient conduction that can cause a change of state in a solid state memory. The particle tracks can be caused by primary cosmic rays entering from outside or primary/secondary cosmic ray particle induced nuclear reactions internal to the device.
Verifying spacecraft avionics reliability in the space flight SEE environment

- **Key concept - Linear Energy Transfer (LET)**
  - LET provides a measure of how much ionization an energetic charged particle produces when passing through matter
  - LET depends on both particle velocity and particle charge

- **Avionics components are tested in ground based charged particle accelerators to determine SEE probability as a function of charged particle LET**
  - Test methods such as ASTM F1192
  - Accelerator beams differ significantly from the space flight environment
  - Components often require extensive modifications to enable testing
  - Some components can’t be tested in this way at all

- **SEE vs. LET data are then combined with the expected space flight charged particle LET environment (including spacecraft shielding mass) to predict (estimate) component SEE rates (failure probability per unit time)**

- **Finally, avionics system SEE rates are predicted from component SEE rates**

The case for supplemental in-flight avionics testing for human interplanetary programs

- Spacecraft avionics systems reliability: ground based test and analysis vs. in-flight experience
  - The limitations of conventional component heavy ion testing are well known and documented and lead to considerable uncertainty in flight system failure rate estimates
  - Uncertainty increases when testing modern complex system-on-a-chip components (e.g. FPGAs)
  - Component level test and analysis often miss integrated system level and configuration effects

- In-flight system level anomalies not identified by ground based test and analysis
  - Examples
    - Cassini solid state recorder multiple bit upsets
    - Cassini single event transients in power switches
    - Hubble stacked memory chip module SEE anomalies
    - Quicksat/Seawinds global positioning system single event latch-ups
    - In-flight Mercury Messenger component SEE rates orders of magnitude higher than predicted

- When unexpected or anomalous events arise, the Spacecraft Operations Flight Support Team (SOFS) must trouble shoot the problem and implement a solution within allowable time constraints
“Test Like You Fly and Fly Like You Test”

  - Systems Principle 6 – Design, build and verify the system employing a “test like you fly, fly like you test” philosophy
  - “Test Like You Fly” is a philosophy which assures that the test environment, configuration, and operations reflect the way the system will be used
    - The closer to the operational environment the test conditions are, the higher the fidelity of the test and the more likely that the test will discover correctable problems in the hardware/software compliment before flight
  - “Fly (operate) Like You Test” is a philosophy which avoids operating the system in an environment, configuration, or way which has not been verified
    - When properly implemented, the system verification process exercises the system, in operational configurations and environments that, to the degree practical, accurately represent the flight environment and operational configurations so that fewer unanticipated problems will occur during flight operations
- Conventional SEE verification using low fidelity testing at the parts level only with subsequent analysis to calculate the expected on-orbit failure rates is clearly NOT a test like you fly and fly like you test approach
  - Explains the many documented testing escapes (i.e. in-flight failure modes not detected during test)
The SEE environment at ISS and in interplanetary space: Environmental Scaling Factors

For charged particle LET values of interest for avionics SEE effects ($> 0.1$ LET units), the annual particle fluence in interplanetary space is greater than the annual particle fluence at ISS. So, for the same charged particle fluence, more testing time will be needed at ISS than in interplanetary space.

Testing Time Scale Factor\(_{\text{LET Threshold}}\) = \(\frac{\text{Annual ISS particle fluence}}{\text{Annual interplanetary particle fluence}}\)

ISS to interplanetary SEE environment testing time scaling factors for a range of LET thresholds

<table>
<thead>
<tr>
<th>LET Threshold * ((\text{MeV cm}^2)/\text{mg})</th>
<th>0.1</th>
<th>1.3</th>
<th>4.0</th>
<th>9.9</th>
<th>20.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Scale Factor**</td>
<td>0.48</td>
<td>0.19</td>
<td>0.21</td>
<td>0.14</td>
<td>0.14</td>
</tr>
<tr>
<td>Maximum Scale Factor</td>
<td>0.97</td>
<td>0.27</td>
<td>0.33</td>
<td>0.30</td>
<td>0.44</td>
</tr>
<tr>
<td>Minimum Scale Factor</td>
<td>0.27</td>
<td>0.13</td>
<td>0.12</td>
<td>0.04</td>
<td>0.05</td>
</tr>
</tbody>
</table>

* Note that as a general rule only those microelectronic devices with thresholds greater than 1 LET unit are useful in high reliability spacecraft avionics systems

** Averages and extremes corresponding to a shielding mass range of 0.8 to 80 g/cm\(^2\) Al
Interplanetary Avionics System Reliability Testing on ISS: Methods and Approach

- Use proven reliability engineering test methods utilizing Bayesian inference
  - MIL-HDBK-338B, Electronic Reliability Design Handbook, Section 8.3
  - NASA/SP-2009-569, Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis, section 8.3
  - Conventional ground based SEE testing (ground up approach) provides the “Bayesian Prior”
    - For example:
      - ASTM Guide F1192-00–Standard guide for the measurement of single event phenomena (SEP) induced by heavy ion irradiating of semiconductor devices [F1192M]
      - 2. JEDEC heavy ion testing guideline [JEDEC HI]
      - 3. ASTM Standard 883: Test Method 1019.5 [1019.5]
  - Alternately, new high energy heavy ion and proton test methods may provide an alternative approach offering considerable potential advantages over the conventional methodology, but require further development at this time

- Note that system architecture and system redundancy determine the reliability requirements imposed on the individual sub-systems (“boxes”) and components
- Step-1: select an architecture likely to meet mission requirements with reasonable box level reliability
Interplanetary Avionics System Reliability Testing on ISS: How would we do that?

• Select an architecture likely to meet mission requirements with reasonable box levels of reliability
  – Mission duration = 3 years = 26,280 hours
  – In mission system maintenance/refurbishment – None
  – System Reliability Function, \( R(t) \geq 90\% \) at \( t = 26,280 \) Hours

• Using standard methods available at http://reliabilityanalyticstoolkit.appspot.com/
  – Compare various parallel redundant system architectures with respect to box/unit MTBF values that will meet the system reliability requirements
  – Box/unit level reliability (MTBF) must be low enough to be testable and verifiable within reasonable schedule and cost constraints

• System architecture results
  – Active parallel redundancy with 3 active units and 6 cold standby units can meet the system requirements box/unit MTBF between 20,000 and 25,000 hours (MTBF\(_{lower}\) with 90% confidence)
  – Active parallel redundancy with all units active cannot meet the system reliability requirements with all units active, even with 9 units
  – Model calculation and box unit level test plans are summarized in the following
Interplanetary Avionics System Reliability Testing on ISS: An example

System Characteristics:
Number of units required for mission success (m): 3
Total number of units (n): 9
Number of cold standby units (n-m): 6
Probability that switch will work correctly: 1
Failure rate (λ) of each unit, failures per million hours (FPMH): 40.00
Mean time between failure (MTBF) of each unit (hours): 25,000
Maintenance interval (T) between system renewal (hours): 26,280
Distribution type: Exponential

Solution:
The system reliability at 26,280 hours is:
\[ R(26,280 \text{ hours}) = 0.96 \]
Effective failure rate of system: 1.60 FPMH
Effective MTBF of system: 623,301 hours
Mean time to failure (MTTF): 58,336 hours.
Testing at ISS: test time and number of test articles to establish an MTBF\textsubscript{lower} (\(\lambda_{\text{upper}}\)) with 90\% confidence

**Inputs:**

Required MTBF: **25,000.0** hours.
Allowable failures: **1**
Confidence: **90\%**

**Solution:**

97,243 total test hours are required, with 1 allowable failure occurring, to demonstrate a unit MTBF of **25,000** hours with **90\%** confidence in LEO

**Testing:**

97,243 total test hours are required corresponding to **5 test articles** at 19,449 hours (2.2 years) each in LEO corresponding to 0.2 x (97,243) = 19,449 hours in cis-lunar space (0.2 is the ISS to IP SEE environment scaling factor determined earlier)

486,215 total LEO test hours are required to demonstrate a 25,000 hour lower MTBF with 90\% confidence in the interplanetary environment implying **25 test articles at 2.2 years each** or **12 test articles at 4.4 years each**
Summary and Conclusions

- Routine cargo missions to ISS several times a year make in-space test and verification of spacecraft avionics systems possible for the first time.

- ISS provides a unique opportunity for spacecraft avionics systems developers to perform comprehensive, “fly like you test and test like you fly” testing:
  - Flight testing on ISS makes it possible to simultaneously evaluate multiple space flight environment effects including: SEE effects, thermal vacuum and microgravity effects, as well as evaluating EDAC, FDIR, and functional interrupt recovery strategies.
  - Overall avionics system reliability can be tested/evaluated in the combined flight environment.
  - Failure modes that escape conventional ground based testing can be identified and corrected early in development.
  - Ultimately the more severe safety and reliability requirements expected for long duration human interplanetary flight can be verified with increased confidence and with reasonable cost and schedule impacts.

- Can the ISS be used as an avionics SEE test platform for supplemental verification of safety critical avionics systems designed for long term operation in interplanetary environments? YES