Paper Session I-C - Avionics Reliability Considerations for Autonomous Reusable Launch Vehicles

J. Ned Yelverton
Principle Engineer, Loral Space Information Systems

Follow this and additional works at: https://commons.erau.edu/space-congress-proceedings

Scholarly Commons Citation
https://commons.erau.edu/space-congress-proceedings/proceedings-1996-33rd/april-23-1996/15

This Event is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in The Space Congress® Proceedings by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.
Avionics Reliability Considerations for Autonomous Reusable Launch Vehicles

J. Ned Yelverton
Principal Engineer
Loral Space Information Systems, Houston, Texas

Abstract

This paper will examine and trade various unique aspects and issues associated with the avionics reliability necessary for autonomous operation of future reusable space launch vehicles.

Introduction and Background

The requirement for unmanned autonomous launch vehicles, such as the currently planned Reusable Launch Vehicle (RLV/X-33), poses interesting problems for the avionics system--where the intelligence must reside to provide the necessary (and essential) automatic operations under all conditions of flight, environments, and anomalous/degraded conditions of the vehicle. The avionics system must be robust from a fault-tolerance point of view, which must include and incorporate new flight/launch rules that will permit a “launch-with-failures” (if project cost goals are to be met).

Key Launch Vehicle Requirements–Avionics Perspective

In order to accommodate “faults-at-launch” conditions, the onboard avionics must be highly redundant, if designed based on classical configurations, which may create a significant cost issue. The alternative is to employ other state-of-the-art techniques for fault recovery or circumvention. This scenario presents a spectrum of solutions that range from traditional replication (redundancy is increased until the fault quantity is adequately covered) up to more sophisticated approaches for reconfiguration using switching of spares and automatic reconfiguration.

In order to fully understand the above reliability requirements, critical phases of the mission must be considered---with launch/boost/ascent and deorbit/reentry/landing generally considered to be the most demanding times, followed closely by in-orbit operations in close proximity (or in contact) with other orbiting structures and vehicles.
The following unique requirements goals may be established for a next generation reuseable launch vehicle:

| • Autonomy                          | • (Total) No Person-in-the-Loop                      |
|                                     | • Intelligence must reside truly On-Board           |
| • Re-Use                           | • Reliable return for rapid turnaround for another mission |
| • Launch-with-Fault (One or more)   | • Start mission with a penalty                      |
|                                     | • L = Launch Faults ( L = 1, 2, ... )               |
| • Mission Fault-Tolerance          | • Two or more with continuation of mission functions|
|                                     | • M = Mission Faults ( M = 2, 3, ... )              |
| • L + M Minimum = 3                | • The sum of launch and mission faults.             |

All of the above requirements will impact avionics system redundancy and reliability in the following ways:

- Must have enough redundancy and/or spares to tolerate the implied (L + M) faults---too much equipment, however, will degrade the results (a diminishing returns issue),

- No person will be actively in the loop to assist in real-time decisions on fault-downs and/or backup switching,

- Cost, weight, and power are impacted if brute force approaches are taken.

**Avionics Reliability Requirements--Implied and Assumed**

The following characteristics will be used in this paper to assess the issues associated with the avionics configuration necessary to perform the launch vehicle mission:

- Launch Vehicle--Success greater than 1 out of 1000 missions --0.999 minimum reliability per mission,
• Avionics reliability to be greater than 0.99999--( 100 X)--Avionics must not contribute to the unreliability of the vehicle,

• \[ L + M = 3 \]

• Typical integrated avionics set--one simplex set (or string) with the following capability,

  1. Simplex--one of each avionics function residing in CPU, I/O, GN&C (including integrated GPS/INS), Air System, Comm, etc.,
  2. Assume a 5 box set for the above---average box MTBF = 25,000 hours,
  3. String failure rate (\( \lambda \)) = ( 5 / 25,000),
  4. String reliability = 0.953 for a 10 day (240 hour) mission.

**Avionics Configuration--Redundancy Assessment**

A fault-masking avionics configuration, implemented with strings of the avionics described in the previous section will provide the following capability:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Faults Covered</th>
<th>Reliability</th>
<th>End Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 String TMR</td>
<td>1</td>
<td>0.994</td>
<td>XOO</td>
</tr>
<tr>
<td>4 String Quad</td>
<td>2</td>
<td>0.9996</td>
<td>XXOO</td>
</tr>
<tr>
<td>5 String Pentad</td>
<td>3</td>
<td>0.99998 (Meets)</td>
<td>XXXOO (O = operational) (X = faulted)</td>
</tr>
</tbody>
</table>

The following conclusions may be drawn from the above analysis:

• Five (5) strings of avionics are required to satisfy the minimum fault coverage requirement (\( L + M \)),

• Five (5) strings will just meet (approximately) the avionics system reliability for the full 240 hour mission---will exceed requirements if the criticality duty-cycle is considered.
Fault-Down Rule Considerations

The previous analysis assumed fault-down to a dual configuration, still operational in a mission abort situation. If the ability to isolate down to simplex is considered, which requires isolation of the faulty unit after a dual miscompare, then the following results:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Fault Quantity</th>
<th>Reliability</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 String TMR</td>
<td>2</td>
<td>0.9999</td>
<td></td>
</tr>
<tr>
<td>4 String Quad</td>
<td>3</td>
<td>0.999995</td>
<td>(Exceeds) Meets L+M Min.</td>
</tr>
</tbody>
</table>

These results show that fault-down to simplex permits implementation with a 4 string (Quad) system—a drop back from 5 to 4 strings. The risk involved with this approach, however, which deviates from transparent fault-masking, is the reliability and time involved to perform the isolation of the faulty unit after the dual miscompare occurs.

Switched Redundancy Considerations

Switched redundancy, based on the following rules, was investigated to determine if improvements could be achieved:

- Always have at least TMR active to mask one fault as it occurs,
- Switch in a new member and drop the faulty unit after each fault,

Results showed that reliability of each configuration was essentially boosted approximately 10 X, effectively achieving an additional “virtual” string. The Quad system could achieve close to the required system reliability of 0.99999:

- Reliability of Quad (3 + 1)= 0.99998 (close to requirement),
- Reliability of Pentad (3 +2)= 0.999998 (exceeding requirement).
Conclusions from analysis of this technique were as follows:

- Improves reliability significantly (spares have near zero failure rate), but *not fault coverage*,

- Carries the risk associated with switching complexity, and the recovery time involved with bringing cold spares into the redundant system.

**Other Considerations**

Numerous other popular fault-tolerance and redundancy methods were examined for compliance with the launch vehicle avionics requirements under consideration. A synopsis of some of these studies is given below:

1. A combination of *Switching and Fault-Down to Simplex*
   - Further enhances reliability, but with no additional fault coverage (essentially not enough physical assets),
   - Adds complexity for managing power switching and isolating single failed units.

2. Fault Containment Regions
   - Increases the average fault coverage by approximately half the number of containment regions,
   - Worst case---no better than straight-line independent strings.

3. Pair-of-Pairs Approaches
   - Technique is based on dual compare--disagreement detection--switch to a standby/backup unit or system,
   - Recovery (switch-over) time is involved, which must be less than the critical recovery time of the control system,
   - Management of switched resources is required,
• Fault coverage is no greater than that for fault masking; reliability is less due to the comparison and switchover hardware.

**Recommendations**

The following recommendations for launch vehicle avionics results from the analyses considered in this paper:

1. An independent/isolated avionic string approach with real-time fault-masking (inherent recovery, inherent isolation, and zero recovery time)--isolated strings simplify configuration for testing, checkout, and health-management purposes,

2. Consider power and reliability enhancements with power switching--will need switching for reduced avionics capability during non-critical mission phases (will not improve fault coverage, however),

**Observations and Conclusions**

With the reliability available from the current (and projected) generation of avionics technology, it appears that system redundancy will be primarily driven by the fault coverage requirements (L + M) and not the system reliability. This is especially true in cases, as in this paper, where the fault coverage is high, and includes inherent faults at the start of the mission. Configuration schemes designed to cover L + M faults will yield resulting system reliability numbers exceeding a requirements level that might otherwise be entirely adequate for the project.