Understanding System Safety: Hazards, Controls, Inhibits, and Independence

Dr. Gerry Shaw
Senior Research Engineer
SRI International
2.3.1 No electronics shall be active during launch to prevent any electrical or RF interference with the launch vehicle and primary payloads...

2.3.2 The CubeSat shall include at least one deployment switch to completely turn off satellite power once actuated.

2.4.2 All deployables such as booms, antennas, and solar panels shall wait to deploy a minimum of 30 minutes after the CubeSat’s deployment switch(es) are activated from P-POD ejection.

2.4.3 RF transmitters greater than 1 mW shall wait a minimum of 30 minutes after the CubeSat’s deployment switch(es) are activated from P-POD ejection.
Compliant Architecture?

- Power
  - Deployment Switch
  - P-POD Door

- "Switch"
  - 30 min Delay Timer

- Transmitter
  - Deployment Release Mechanism
Assess Hazard

<table>
<thead>
<tr>
<th>Hazard Severity</th>
<th>Potential Consequences</th>
<th>Probability*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I - Catastrophic</td>
<td>May cause death.</td>
<td>Data is never recoverable or primary program objectives are lost.</td>
</tr>
<tr>
<td></td>
<td>&gt; 1,000,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt; 4 months</td>
<td></td>
</tr>
<tr>
<td>II - Critical</td>
<td>May cause severe injury or severe occupational illness.</td>
<td>May cause repeat of test program.</td>
</tr>
<tr>
<td></td>
<td>200,000 to 1,000,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 weeks to 4 months</td>
<td></td>
</tr>
<tr>
<td>III - Marginal</td>
<td>May cause minor injury or minor occupational illness.</td>
<td>May cause repeat of test period.</td>
</tr>
<tr>
<td></td>
<td>10,000 to 200,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 Day to 2 Weeks</td>
<td></td>
</tr>
<tr>
<td>IV - Negligible</td>
<td>Will not result in injury or occupational illness.</td>
<td>May cause repeat of data point, or data may require minor manipulation or computer rerun.</td>
</tr>
<tr>
<td></td>
<td>&lt; 10,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt; 1 Day</td>
<td></td>
</tr>
</tbody>
</table>

Risk Priority: [Unacceptable, Waiver required, Operation permissible]

*Probability refers to the probability that the potential consequence will occur in the life cycle of the system (test/activity/operation).
Use the following list to determine the appropriate Risk Level.

<table>
<thead>
<tr>
<th>Threshold Level</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Frequent</td>
<td>8X10^-2</td>
</tr>
<tr>
<td>B Reasonably probable</td>
<td>8X10^-3</td>
</tr>
<tr>
<td>C Occasional</td>
<td>8X10^-4</td>
</tr>
<tr>
<td>D Remote</td>
<td>8X10^-5</td>
</tr>
<tr>
<td>E Extremely Improbable</td>
<td>8X10^-6</td>
</tr>
</tbody>
</table>

- Value: 3X10^-1
- Specific Individual Item: Likely to occur repeatedly
- Fleet or Inventory: Continuously experienced
- Value: 3X10^-2
- Specific Individual Item: Likely to occur several times
- Fleet or Inventory: Will occur frequently
- Value: 3X10^-3
- Specific Individual Item: Likely to occur sometime
- Fleet or Inventory: Will occur several times
- Value: 3X10^-4
- Specific Individual Item: Unlikely to occur, but possible
- Fleet or Inventory: Unlikely, but can reasonably be expected to occur
- Value: 3X10^-5
- Specific Individual Item: Very unlikely to occur, but still possible.
- Fleet or Inventory: Unlikely to occur, but possible

AFSPCMAN 91-710, Vol. 1, Figure 3-2
Hazard Mitigation

• **Hazard Control Precedence...**
  – Change design to eliminate or minimize hazards
    • For example: Reduce transmitter power
  – Add engineered safety features
  – **Incorporate safety devices (inhibits)**
    • For example: Introduce Inhibits
  – Provide warning devices
  – Develop procedures and training

• **Inhibits**
  – Physical devices that interrupt the “power path” needed to turn on a potentially hazardous device
Two independent inhibits
  • Increased safety
  • Double jeopardy for power on
Two Series Deployment Switches

- Two independent inhibits
  - Increased safety
  - Still single inhibit for power on

Diagram:
- Power
  - Deployment Switch
  - Inhibit
  - "Switch"
  - Transmitter

- P-POD Door
- Photo Cell(s) or Solar Panel
- 30 min Delay Timer
- Deployment Release Mechanism
Transmitter Requires Additional Inhibit Inhibit

Two independent inhibits for deployables
Three independent inhibits for transmitter
Still single inhibit for power on

Power

Deployment Switch
P-POD Door

Inhibit
Photo Cell(s) or Solar Panel

“Switch”
30 min Delay Timer

Deployment Release Mechanism

Inhibit

Transmitter

Confirm Antenna Fully Deployed (Good Idea) or Ground Command
No Single Point of Failure

- Multiple inhibits controlled by a single processor could have common failure mode.

Diagram:
- Processor
  - Control 1
  - Control 2
  - Inhibit
  - Inhibit
  - Potentially Hazardous Device

Independent and No SPOF
Summary

1. Identify hazards and causal factors using a systematic approach.
2. Assess severity and probability of hazard mishap risk.
3. Identify mitigation measures (safety design requirements).
   • Influence design, order of precedence
4. Reduce hazard risk to an acceptable level.
   • Make inhibits work for both safety and mission assurance
Contacts:
Dr. Gerry Shaw
gerald.shaw@sri.com
(805) 542-9330 x-108

Dr. Mark Tinkle
mark.tinkle@sri.com
(805) 542-9330 x-106