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?
Assess Hazard

### Hazard Severity

<table>
<thead>
<tr>
<th>Category</th>
<th>Personnel Injury</th>
<th>Equipment Loss ($)</th>
<th>Unit Downtime</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Catastrophic</td>
<td>May cause death.</td>
<td>&gt; 1,000,000</td>
<td>A</td>
</tr>
<tr>
<td>II</td>
<td>Critical</td>
<td>May cause severe injury or severe occupational illness.</td>
<td>200,000 to 1,000,000</td>
<td>B</td>
</tr>
<tr>
<td>III</td>
<td>Marginal</td>
<td>May cause minor injury or minor occupational illness.</td>
<td>10,000 to 200,000</td>
<td>C</td>
</tr>
<tr>
<td>IV</td>
<td>Negligible</td>
<td>Will not result in injury or occupational illness.</td>
<td>&lt; 10,000</td>
<td>D</td>
</tr>
</tbody>
</table>

### Probability

- **A**: Data is never recoverable or primary program objectives are lost.
- **B**: May cause repeat of test program.
- **C**: May cause repeat of test period.
- **D**: May cause repeat of data point, or data may require minor manipulation or computer rerun.

### Risk Priority

- **Unacceptable**: Requires a waiver before the system can be operated.
- **Waiver required**: Must be waived before the system can be operated.
- **Operation permissible**: System is operated with a waiver, but it is an unacceptable risk.

### Threshold Level and Probability

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
<th>Specific Individual Item</th>
<th>Fleet or Inventory***</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>8X10^{-2}</td>
<td>Likely to occur repeatedly</td>
<td>Continuously experienced</td>
</tr>
<tr>
<td>B</td>
<td>8X10^{-3}</td>
<td>Likely to occur several times</td>
<td>Will occur frequently</td>
</tr>
<tr>
<td>C</td>
<td>8X10^{-4}</td>
<td>Likely to occur sometime</td>
<td>Will occur several times</td>
</tr>
<tr>
<td>D</td>
<td>8X10^{-5}</td>
<td>Unlikely to occur, but possible</td>
<td>Unlikely, but can reasonably be expected to occur</td>
</tr>
<tr>
<td>E</td>
<td>3X10^{-5}</td>
<td>Very unlikely to occur, but still possible.</td>
<td>Unlikely to occur, but possible</td>
</tr>
</tbody>
</table>

---

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 Series Deployment Switches

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

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

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

Legend:
- Independent and No SPOF
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