NASA Hazard Analysis Process

George Deckert
Johnson Space Center
Safety, Reliability and Mission Assurance Directorate
Significant Incidents and Close Calls in Human Spaceflight

A Product of the JSC S&MA Flight Safety Office

The Significant Incidents and Close Calls in Human Spaceflight is primarily focused on human spaceflight incidents that have occurred while a crew was aboard a space vehicle. It includes suborbital, orbital, and lunar missions. The low-gravity facility events and two atmospheric flight events are included due to the significance of the events to spaceflight. The propulsion system failure of the SR-71 and X-15 in Russia occurred prior to the loss of the Apollo 10 and 11 in 1969 and could have served as a lesson learned had it been known in the US. The EMU fire resulted in the redesign of the EMU and heightened awareness of design and materials selection for man-rated systems using a pure CO2 environment. The U-2/Skye drive accident occurred during the development of the space shuttle and yielded personnel engineering lessons learned. The SST engine is the highest and fastest vehicle breakup on record that was survivable and it represents the demonstrated level of crew survival with currently fielded technologies. Note: This document is in work in progress. It is continually under review and frequently updated. Please direct comments and questions to the Flight Safety Office contacts at right.
Subsystem Safety Engineering Through the Project Life Cycle

**Work Authorization**
- Kick off
- Work Authorization

**Mission Definition**
- Reviews
- Mission Definition Review

**System Requirements**
- Review
- System Requirements Review

**Preliminary Design**
- Review
- Preliminary Design Review

**Critical Design**
- Review
- Critical Design Review

**Test Readiness**
- Reviews
- Test Readiness Reviews

**Acceptance Readiness**
- Reviews
- Acceptance Readiness Reviews

**Operational Readiness**
- Review
- Operational Readiness Review

**System Delivery**
- Delivery
- System Delivery

**Production Performance**
- Reviews
- Production Performance Reviews

---

**Pre Phase A & Phase A**
- Formulation

**Concept Development**
- Requirements
- Safety
- Reliability
- Maintainability
- Quality
- Supportability
- Specifications
- & Standards
- Program or Project Plans
- PQA
- RIDs

**System Definition**
- Requirements Analysis
- Safety Data Package
- FMEA
- Drawings
- Verification Plans
- Prototype Concept
- Analysis & Candidate Selection List
- PQA
- QA Audit
- RIDs

**Prototype & Prelim Design**
- Requirements
- Analyses
- Safety Data Package
- FMEA
- Drawings
- Verification Plans
- Prototype Concept
- Analysis & Candidate Selection List
- PQA
- QA Audit
- RIDs

**Final Design**
- Safety Data Package
- FMEA
- Drawings
- Verification Plans
- Prototype Concept
- Analysis & Candidate Selection List
- PQA
- QA Audit
- RIDs

**Fabrication**
- Inspection
- QA (Work Auth)
- Test Plans & Procedures
- QA Audit
- PRACA
- PQA
- GIDEP ALERTS

**Integration & System Test**
- System Test Report
- Certification Data Package
- Final Safety Data Package
- FMEA/CIL
- Verification & Validation
- QA Audit
- PRACA
- GIDEP ALERTS

**Deployment & Acceptance**
- Configuration Items
- Acceptance Data Packages
- GIDEP ALERTS
- Lessons Learned
- MCRs
- QA Audit
- PRACA
- RIDs

**Operation & Maintenance**
- Change Requests
- Problem Resolution
- Training
- Flight Rules & Procedures
- CoFR
- Mission Operations
- SPIR

**Retirement/Disposal**
- Retirement Plan
- System Closeout Report
- Materials Disposition Report
- Lessons Learned

---

**Risk Management**

**Preliminary Hazard Analysis**

**Integrated Hazards Analysis**

**Subsystems Hazards Analysis**

**Element Hazards Analysis**

**Human Factor Analysis**

**S/W Hazards Analysis**

**Hazard Report Development**

---

**Hazards Report Maintenance/ Risk Analysis**
The Risk Informed Design Process

- The process is a continuous process throughout the lifecycle of the Project
- At each design and verification cycle, work to reduce the risk drivers
  - Focus on the Top Drivers to maximize impact
- When new drivers emerge (new cycles) as Top Drivers, work those drivers
- Key decision points emerge at various program milestones (e.g. Achievability)

**NASA Risk informed Design Process**
- Use of PRA, Hazard Analysis, and FMEA
- Use of engineering judgment and analysis
- Use of Operational judgment and analysis
Types of NASA Hazard Analysis

• Preliminary Hazard Analysis
• Subsystem Hazard Analysis
• Element Hazard Analysis
• Operating and Support Hazard Analysis
• Software Hazard Analysis
• Integrated Hazard Analysis
• Functional Hazard Analysis
The PHA is the initial effort in hazard analysis during the early design phases that identifies top level hazards and controls, provides a first look at the system risk, and provides the foundation for future analyses. It is based on the best available data. Sources for data include but are not limited to: system description documents, system diagrams, mission descriptions, operational concepts, functional analysis/architecture documents, Functional Flow Block Diagrams (FFBDs), mishap data from similar systems, and lessons learned from other projects. The PHA identifies and evaluates the hazards and hazardous events associated with the proposed design or functions for potential hazard severity, probability, time of exposure, and hazard classification. Design controls, software controls, operational controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level should be considered and documented.
Hazard Analysis Process

• Identify hazardous conditions, events or states
• Identify the effect of the hazardous state
• Identify severity of the effect
• Identify all potential causes of the hazardous states
• Identify controls for each of the hazard causes
• Identify likelihood of each cause
• Identify verification strategies for the controls
• Track verification to closure
Identify Hazardous Conditions

• Basically this is a brainstorming exercise!
• What is inherently dangerous about the operation of your system?
  – Standard hazard lists
  – Historical experience/documentation from legacy systems
  – Your engineering training and experience
Consider all Interfaces

My Subsystem

Other Subsystems
Example

- ISS Crew Transport Mission
  - Launch a crew to the International Space Station
  - Stay docked to the Space Station for 6 months
  - Return the crew to Earth and land in the water
Work a Preliminary Hazard List

• Identify the hazards for this mission.
<table>
<thead>
<tr>
<th>Left Column</th>
<th>Right Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collision or Impacts</td>
<td>Implosion/Loss of Pressure</td>
</tr>
<tr>
<td>Loss of Control</td>
<td>High Pressure Sources</td>
</tr>
<tr>
<td>Contamination</td>
<td>Loss of Structural Integrity</td>
</tr>
<tr>
<td>Corrosion</td>
<td>Mechanical</td>
</tr>
<tr>
<td>Electrical Discharge/Shock</td>
<td>Loss of Critical Function</td>
</tr>
<tr>
<td>Environmental/Weather</td>
<td>Loss of Safe Return Capability</td>
</tr>
<tr>
<td>Temperature Extremes</td>
<td>Loss of Habitable Environment</td>
</tr>
<tr>
<td>Gravitational Forces</td>
<td>Pathological/Physiological/Psychological</td>
</tr>
<tr>
<td>Electromagnetic Interference</td>
<td>Inadequate HF Engineering</td>
</tr>
<tr>
<td>Radiation</td>
<td>Lasers</td>
</tr>
<tr>
<td>Explosion</td>
<td>Utility Outages</td>
</tr>
<tr>
<td>Fire/Overheat</td>
<td>Common Cause Failures</td>
</tr>
<tr>
<td>Flight Termination Systems</td>
<td></td>
</tr>
</tbody>
</table>
• Hazard analysis results in the identification of risks and the means of controlling or eliminating them. Hazard analysis also quantifies the risk for the Program/Project Manager.
Final Thoughts

• Hazard analysis is structured process to
  – Identify risk
  – Classify risk
  – Manage risk

• Hazard analysis is not an exact science
  – Relies on engineering expertise and engineering judgment
  – Requires rationale to justify hazard classification

• Hazard analysis is an important tool in
  – Design Process
  – Requirements Validation
  – Risk Management