Precursor Analysis for Flight- and Ground-Based Anomaly Risk Significance Determination

Frank Groen, PhD
NASA Office of Safety and Mission Assurance

Presented at
Space System Risk Management Symposium
El Segundo CA, April 2010
Need for Precursor Analysis

- CAIB Final Report (October 2003)
  - Section 6.1: “The Board notes that although there is a process for conducting hazard analyses when the system is designed and a process for re-evaluating them when a design is changed or the component is replaced, no process addresses the need to update a hazard analysis when anomalies occur.”

  - Section 7.1: “Signals of potential danger, anomalies, and critical information should, in principle, surface in the hazard identification process and be tracked with risk assessments supported by engineering analyses.”

  - Finding 7.4-5: “Risk information and data from hazard analyses are not communicated effectively to the risk assessment and mission assurance processes. The Board could not find adequate application of a process, database, or metric analysis tool that took an integrated, systemic view of the entire Space Shuttle system.”

- 2006 ASAP Annual Report in regards to Safety Management
  - “the ASAP found that ...the Agency, could better gauge the likelihood of losses by developing leading indicators, rather than continuing to depend on lagging indicators.”
"Swiss Cheese" Concept of Precursor Analysis

- Ordinarily, accidents are prevented by a combination of barriers (human and hardware system features to prevent accidents)
  - Some holes due to active failures
  - Other holes due to latent conditions (resident "pathogens")
  - Successful layam of defences, barriers and safeguards

- Complete pathway through cheese represents accident
- Precursor conceived as partial pathway through the holes in Swiss cheese
- Precursor analysis then corresponds to learning about existence and size of holes
"Precursor" Definition

- Definition of a "precursor"
  - An indication of a problem with the potential to recur with more severe consequences

- Key Attributes:
  - Observation indicates some failure mechanism
  - Same mechanism could occur again
  - The consequences could be more severe than what has been experienced
Anomaliess

Challenger
- Severe Burn-through, ET containment compromised, Loss of Shuttle
- Debris impacts on thermal protection system
- Frequent Containment Air Filter Replacements
- O-ring blow-by
- Other Observed Anomalies

Columbia
- Severe RCC Impact, Loss of Shuttle on re-entry

Davis-Besse NPP
- Significant Vessel Head Erosion
- Large Loss of Coolant Accident

(Potential) Failures

How do we focus on risk-significant anomalies?
Examples of Types of Precursors

- A near-miss because of chance or an opportune mitigation
- Faults that can become failure conditions without correction
- Unexpected trend in test, operation, or maintenance
- Unexpected effects from aging of equipment
- Common causes of faults or deteriorations
Accident Precursor Analysis

- Establishes a systematic process for evaluation of flight and test anomalies
  - Risk-based evaluation of failure mechanisms
  - Triggered by actual flight/test experience
  - Emphasizes ‘imagination’ through generalization

- Provides insight into safety performance
  - Identifies safety-related system vulnerabilities
  - Indicates trends in safety performance

- Makes safety analysis more experience-based
  - Triggers review/modification of safety models based on analysis findings
    - Completeness of represented failure modes
    - Failure probabilities and influencing factors
Real World vs. Models

Our Systems
- Shuttle
- ISS
- Robotic Missions
- Ground Facilities

Safety and Performance Model
- PRA
- Reliability Model
- Trending Model
- Accident Precursor Model
- Others

Collection and Analysis of Operational Data (e.g., failure, faults)
Supports Development of Models

Operational Off-Nominal Data
- In-flight Anomalies
- Non-conformance cases
- Failures
- Faults
- Others

Results of the Model
- Predicted System Performance
- Trends and Temporal Behavior
- Risk Importance
- Risk/Failure Significance Determination
- Others

- Good Fit? Or Not?

Updating the Model based on Experience

Management Decisions and Actions

Risk Information Input

APA Allows us to Improve the Fidelity & Accuracy of our Models

Feedback

NASA
Overview of NASA’s Accident Precursor Analysis
Technical Approach
Historically, precursor analysis has been focused on failures, e.g., at Nuclear Regulatory Commission.

NASA process extends focus to anomalies:
- NASA's databases contain mostly anomalies (a defect, fault, or other deviation)
- NASA has a stronger incentive to prevent any failure due to fewer barriers in its space systems

Operational definition of precursors:
Anomalies that upon evaluation are determined to indicate a failure mechanism that may pose a significant degree of risk.
NASA APA Process

Anomalies

Screening and Dispositioning

Screen Yes

Dispositioning
Grade the potential impacts to safety

Generalization
Apply the mechanism to different circumstances

No

No Further Action

Analysis

Risk Modeling
Quantify the impacts

Results

Findings
Complete results, reconciling the model with reality

Observation & Trending

No Further Action
Anomaly Dispositioning Model

Mechanism active within subsystem or component
Potential for Failure Conditions of Concern
Potential for Severe Consequences
Problem Potential Index

Other failure times
Other systems
Other locations on the affected system
Larger fault magnitude
Anomaly failure mechanism

GPFs

4
7
9
5
Disposition Pathways

- Anomalies without obvious risk- or reliability implications are removed from consideration using rules-of-thumb.

- Failure mechanisms of screened-in anomalies are determined and generalized.

- Dispositioning is based on:
  - Generalized problem potential
  - Evidence caliber
Probabilistic Analysis

- Parametric Probabilistic Modeling & Risk Significance Assessment
  - Quantify the risk potential for anomalies and GPFs dispositioned for Risk Modeling
  - Provides a rigorous assessment of the quantified risk significance of the failure mechanism acting within the system while also highlighting parametric uncertainties of the accident sequences that should be further investigated

Scenario Development for Events Dispositioned for Risk Modeling

PPM Results

Anomaly Risk Importance & Parameter Vulnerability Analysis
Example Space Shuttle Working Session Results

<table>
<thead>
<tr>
<th>Year</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missions</td>
<td>STS-114</td>
<td>STS-116, STS-115, STS-121</td>
<td>STS-120, STS-118, STS-117</td>
<td>STS-124, STS-123, STS-122</td>
</tr>
</tbody>
</table>

Observation & Trending

Rule-Based Screen Out
Closing Remarks

- Accident Precursor Analysis (APA) has been used by other govt agencies with positive results (e.g., NRC)
- Intended to be applied outside the normal problem resolution cycle
- Development of NASA APA methodology will continue in 2010