NASA’s Accident Precursor Analysis Process and the International Space Station

Trilateral Safety and Mission Assurance Conference
NASA Safety Center, Cleveland, Ohio, USA, on
October 26-27, 2010

Frank Groen  NASA/HQ
Michael Lutomski  NASA/JSC
Purpose:
1. Present an overview of Precursor Analysis being implemented at NASA
2. Present a summary completed Precursor Pilots conducted and future plans

Agenda:
- Background
  » Need for Precursor
  » Definition of a Precursor
- What is Precursor Analysis?
- Pilot Precursor Analysis Summary
- Summary & Conclusion
- Future Work
The Need for Precursor

• CAIB Final Report (October 2003)
  - 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.”

• 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.”

• NPR 8715.3C, “NASA General Safety Program Requirements” (March 2008)
  - 2.5.2.2 System engineers shall:
    » d. Ensure that the system safety models are developed in an iterative process to allow model expansion, model updating, and model integration as the design evolves and operational experience is acquired (Requirement).
    » Note: Relevant leading-indicator (or precursor) events should be documented and evaluated for their impact on the system safety analyses assumptions. Trending of these precursor events should be conducted and contrasted to applicable PMs.

  - 2.5.4.1 Project managers shall ensure that the performance attributes and precursors that are identified as being important indicators of system safety are monitored (Requirement).
Background

• Definition of a “precursor”
  – An indication of a problem with the potential to recur with more severe consequences

• Key Attributes:
  – Observation (IFI, PRACA) indicates some “failure mechanism”
  – Same mechanism could occur again
  – The consequences could be more severe than what has been experienced
Columbia accident was actually preceded by a direct accident precursor, **STS-45**. Post flight inspection of the right Reinforced Carbon-Carbon leading edge found two gouges.

Corrective Action Taken: Panel Replaced

- This solved the immediate condition, but did not eliminate the mechanism for more dire consequences
Operational Definition of Precursor

- 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
Background

- **Examples of Precursors**
  - A near-miss because of chance or an opportune mitigation
  - Faults that without correction can lead to severe outcomes
  - Unexpected trend in test or operational data
  - Reduced repair/maintenance effectiveness
  - Unexpected effects from aging of equipment
  - Common causes of faults or deteriorations
What is Precursor Analysis?

- Evaluates IFI (In-Flight Investigation) and PRACA (Problem Reporting and Corrective Action) data to identify unrecognized accident potential or underappreciated vulnerabilities, so they can be addressed/mitigated in a timely manner
  - i.e. looking at your operating data, performance, and experience

- Precursor analysis focuses on aspects of reality that need attention by decision-makers
  - Conditions whose risk potential is not understood in current models (e.g., O-rings, External Tank debris, potential for vessel head to be corroded from the outside)
  - Performance issues whose potential is understood in principle, but whose risk-significance is not
Real World vs. Models

Systems / Operational Practices

Modeling / Analysis

Safety and Performance Model

Hazard Analysis / Reports
Engineering Analysis
Risk / Reliability Models / PRA / and others

Risk-Informed Safety Case

Performance Allocation
Implied Resource Allocation
Performance Commitments
Processes
Input to Risk Management

Management Decisions and Actions

Organizational Learning

Operational Off-Nominal Data

In-flight Anomalies
Non-conformance cases
Failures
Faults
Others

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

Updating the model based on new hazard analysis and on experience

Actual Performance
Predicted Performance

Actual Performance vs. Predicted Performance

Performance Allocation
Implied Resource Allocation
Performance Commitments
Processes
Input to Risk Management

Risk Information Input
What is Precursor Analysis?

- **Precursor Analysis**
  - Screens observed anomalies for need to perform evaluation
  - Evaluates and dispositions events into three categories
  - Performs detailed analysis of selected anomalies

- Makes risk analysis more experience-based

“A failure mechanism that is benign when it occurs under one set of circumstances may not be benign under another.”
Pilot Precursor Summaries

• **Objective**
  - Exercise the Accident Precursor Analysis (APA) Process developed for the ISS

• **Two Pilot sessions were held in 2010**

• **March 2010** - the Electrical Power System (EPS)

• **August 2010** – Communications and Tracking (C&T) along with Command and Data Handling (C&DH)
  - 1.5 days dedicated to anomaly review and generalization
  - 1.5 days dedicated to grading of anomalous conditions
  - Constrained focus of session to the respective system anomalies and did not investigate across all ISS systems
Anomaly Review Results

- A caseload of 40 EPS non-conformance records was produced for the working session and all records were reviewed.

- Many records, however, were screened out from further APA evaluation.
Generalization Results

• Of the 28 Anomalies which were fully reviewed, 15 Generalized Potential Failures (GPFs) were created
  – Total of 33 anomalous conditions (both observed and postulated)
Example Walk-Through Diagram of an ISS Anomaly

**Observed Anomaly**
Ungrounded Connectors on Jumper W3301P1. Jumpers were designed without a grounded backshell; original cables needed grounded backshell. Design flaw exists in some IVA and EVA cases.

**Failure Mechanism**
Design Flaw

**Component Type**
Jumper Cables with Ungrounded Backshell

---

**Observed Anomaly**
Failure Condition of Concern: possibility for electric shock to a crew member (>32V, 3A) during nominal activities

- **GPF #1**
Failure Condition of Concern: possibility for electric shock to a crew member (>32V, 3A) during IVA maintenance

  - **Recommended for further evaluation**

- **GPF #2**
Failure Condition of Concern: possibility for molten metal generation to occur during EVA

  - **Recommended for further evaluation**

---

**Evaluation & Grading**

**Failure Condition Index**
Graded unexpected that a ungrounded jumper cable could cause electric shock to a crew member during IVA maintenance

**Conditional Consequence Index**
Graded probable that electric shock to crew could cause loss of crew

**Failure Condition Index**
Graded unlikely that a ungrounded jumper cable could cause molten metal generation during EVA

**Conditional Consequence Index**
Graded probable that generation of molten metal on EVA could cause loss of crew

---

**Recommended Further Action**

- **None**

- **Risk Modeling**

- **Observation & Trending**
Grading Results (cont)

- All Anomalous Conditions Recommended for Evaluation

![Graph showing potential problem indices for anomalous conditions. The x-axis represents the anomalous condition number, and the y-axis represents the potential problem index. The graph includes bars for each condition, with red bars indicating risk modeling threshold, yellow bars indicating observation & trending threshold, and green bars indicating other conditions. The highest risk conditions are highlighted.]
Results Summary

Process completed for 40 anomalies over ~3 days

- Insufficient information/Acceptance Test/Non-Anomaly Records

Of those 40 records, 28 anomalies were not screened from further evaluation

- 28 evaluated
- 15 GPFs created from 28 anomalies

- 15 recommended for grading
  - 3 recommended for Risk Modeling
  - 3 recommended for Observation & Trending
  - 9 deemed low risk requiring no further analysis
  - 3 had consequences outside of the evaluated system and the expertise of the session.
Results of Screening Criteria

• 1 screen identified
  – Screen out records recorded during acceptance testing
  – Requires search in the “detected during field” for “acceptance” or “ATP”
  – Only applies to PRACA reports

• Other areas for potential screens did not return results
  – Both “open” and “closed” records had sufficient information to complete generalization
  – The type of report (IFI or PRACA) did not reflect any non-applicability to the APA process
  – Records recorded both “on-orbit” as well as at NASA or contractor facilities were found sufficient to generate GPFs
Summary & Conclusion

- 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

- Establishes a foundation for experience-based analysis and trending of actual events from ISS, and Exploration technology demonstrators, and testing to help build more reliable and safer systems.

- Timely implementation provides the possibility of completely avoiding these events
• Successfully demonstrated that Precursor Analysis is implementable on the ISS

• Both PRACA and IFI records were evaluated, and both provided valid risk information to support the process

• ISS experts noted that the Precursor exercise gave them a different perspective on the anomalies reviewed
Future Work

- Future Work
  - Have made the Precursor Analysis part of the Fiscal Year 2011 baseline work plan
Back-up
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
Well-Known Precursors

Anomalies

- Challenger: O-ring blow-by, Debris impacts on thermal protection system, Frequent Containment Air Filter Replacements, Other Observed Anomalies

- Columbia: Severe Burn-through, ET containment compromised, Loss of Shuttle

- Davis-Besse NPP: Severe RCC Impact, Loss of Shuttle on re-entry, Significant Vessel Head Erosion, Large Loss of Coolant Accident

How do we focus on risk-significant anomalies?