Root Causes and Their Analysis at NASA

Process Overview and Examples
2020
Kristie French
NASA Safety Center

This and previous presentations are archived at https://sma.nasa.gov/news/safety-messages.
NASA Root Cause Analysis

• Since the beginning, NASA has had mishaps

• March 16, 1966: Gemini VIII mission abort:
  – Experienced rotation during dock to Agena
  – Unable to perform Extravehicular Activities
  – MI 8621.1 NASA Mishap Investigation Procedure, April 1966

• January 27, 1967: Apollo 1 fire
  – Known issues (Phillips Report)
  – Schedule
  – Systems engineering
  – Insight/oversight
NASA Root Cause Analysis

- Standardized NASA process for Root Cause Analysis (RCA) and documented in NPR 8621.1 in 2004

- **NASA Root Cause Analysis** is defined as a systematic and structured evaluation method that identifies the Proximate, Intermediate, and Root Causes for an undesired outcome; Proximate Causes are easier to discover

- NASA developed a **five-step process** to evaluate mishaps in a broad, comprehensive manner

- Over **500 NASA** teammates have been trained, as well as members of other government Agencies (ex. Army, Navy, Air Force, Occupational Safety and Health Administration, National Transportation Safety Board)

- **NASA Office of Safety and Mission Assurance** and the **NASA Safety Center** developed a software to support the process and provide RCA expertise throughout the Agency

- Certain underlying issues, Root Causes, we still find today
Common Root Causes of NASA Mishaps

• Schedule slip:
  – WB-57 Runway Departure, March 5, 2019
    • Major inspection: Two years vs. eight months
  – Commercial Crew Program
    • Software development: Years vs. months
  – Allows for personnel changes, loss of program knowledge, leadership changes, changes in priorities

• Schedule pressure:
  – DART, April 15, 2005
    • Testing skipped
    • Accepted less than adequate quality
  – Apollo 1
  – Shuttle
  – Allows for decisions made without account for risk
Common Root Causes of NASA Mishaps

• Confidence in heritage hardware:
  – Genesis (2004)-Stardust
  – DART-Pegasus
  – Must understand the:
    • Assumptions
    • Uses
    • Risks

• Systems engineering issues:
  – DART: System functions not understood
  – Genesis: Verification requirements
  – Commercial Crew Program
  – Must understand the whole system and functions to make informed decisions and understand the change effects on system

• Mismatch of talent:
  – Genesis: Crucial test skipped
  – Must ensure our employees are prepared for the job; NASA has a can do attitude and we have an excellent team, but we can’t set them up for failure; use NASA Engineering and Safety Center Subject Matter Experts
Common Root Causes of NASA Mishaps

• Insight/oversight:
  - Balloon mishap (2010):
    • Flow down of requirements
    • Implementation of safety requirements
    • Follow through of Corrective Actions
  - Must understand technical risks and have clear define responsibilities
  - Nature of NASA’s role; how do we identify the right allocation of resources
  - Base on hazard levels, but must not be complacent and be bit by the “unknown unknowns”

• Self-stifling (Anti-Edith Syndrome):
  - DART:
    • Assumed communications International Traffic in Arms Regulations
    • Assumed resources more limited than they were
  - NASA is success oriented; we do more with less if we have to
  - Be Edith: speak up, test the assumed limits and boundaries, allow decisions to be made, make sure risk is accepted at the right level
Conclusions

• NASA RCA identifies what, how, and why systemic problems occur

• **Underlying organizational causes (Root Causes)** are more difficult to identify; if not corrected, they will continue to create similar types of problems

• Learn from the past:
  – Practice effective systems engineering
  – Understand assumptions and risks
  – Speak up

Without identifying and fixing the **systemic organizational problems**, the chance of repeat is significant.

*Note: Available training and definitions are provided in the backup slides*
Backup
NASA Mishap Training

Online:
- SMA-002-11 NASA Interim Response Team Training
- SMA-002-07 Overview of Mishap Investigation*
- SMA-002-08 Mishap Investigation Roles and Responsibilities*
- SMA-002-09 Completing the Investigation and Mishap Report*
- SMA-002-10 Introduction to Root Cause Analysis*
- SMA-001-07 Human Factors*
- SMA-002-12 Root Cause Analysis Tool
- SMA-002-13 Mishap Investigation Board (MIB) Chair Training
  * prerequisites for classroom training

Classroom (must attend all of class to receive credit):
- SMA-SAFE-OSMA-4003 NASA Root Cause Analysis (preferred)
- SMA-SAFE-OSMA-4004 Human Factors in Mishap Investigation (preferred)

Note:
- SMA-002-14 NASA Root Cause Analysis (may substitute for classroom training SMA-SAFE-OSMA-4003)
- SMA-002-15 NASA Human Factors in Mishap Investigation (may substitute for SMA-SAFE-OSMA-4004)
- Alternate RCA and Human Factors professional training may be submitted for substitution consideration
- NASAHFACS SMA-SAFE-OSMA-4009
NASA Definitions (in RCA Process Order from NPR 8621.1C)

• **Undesired Outcome**: “… the loss that determined the mishap classification (i.e., property damage, mission failure, fatality, permanent disability, lost-time case, or first-aid case).”

• **Proximate Cause**: “The event that occurred, including any conditions existing immediately before the *undesired outcome*, directly resulted in its occurrence, and if eliminated or modified, would have prevented it. Also known as direct cause.”

• **Intermediate Cause**: “An event or condition that existed before the *proximate cause*, directly resulted in its occurrence, and if eliminated or modified, would have prevented the proximate cause from occurring.”

• **Contributing Factor**: “An event or condition that may have contributed to the occurrence of an *undesired outcome*, but if eliminated or modified, would not on its own have prevented the occurrence.”
Organizational Factor: “Any operational or management structural entity that exerts control over the system at any stage in its life cycle including, but not limited to, the system's concept development, design, fabrication, test, maintenance, operation, and disposal—for example, resource management (budget, staff, training); policy (content, implementation, verification); and management decisions.”

Root Cause: “An event or condition, primarily associated with organizational factors, which existed before the intermediate cause and directly resulted in its occurrence (indirectly caused or contributed to the proximate cause and subsequent undesired outcome) and, if eliminated or modified, would have prevented the intermediate cause from occurring and the undesired outcome. Typically, multiple causes contribute to an undesired outcome. In the absence of a prevalent organizational factor, the root cause may be identified as undetermined.”

Minimal Cut Set: A smallest combination of basic events whose occurrence results in the occurrence of the top event of a fault tree.

Types of Recommendations in Order of Effectiveness
1. Eliminate hazards
2. Minimize likelihood hazard will reach the target (barriers and controls)
3. Minimize the worst case effect (improve amelioration, strengthen the target)
4. Provide warnings, when residual risk still exists
RCA Process for Mishaps at NASA

1. Define a single Undesired Outcome, i.e., “NASA astronaut nearly suffered fatal injuries”:
   - Identify what is known and unknown to determine what data (evidence) to collect

2. Build a timeline of conditions and events preceding the Undesired Outcome; identify Proximate Causes from the timeline using the cause test (Precedence, Necessary, and Sufficient)

3. Brainstorm using a wide (not deep) fault tree to examine all possible scenarios for the Proximate Causes:
   - Where refuting data exists, rule out those scenarios (trim the tree); absence of evidence is not evidence of absence: May need to find additional evidence
   - Continue asking why until a stopping rule is reached:
     a) Run out of evidence
        OR
     b) The factor is outside NASA control
        OR
     c) Reached the organizational level (Administrator, Mission Directorate/Program, or Center Director) for that Branch
4. Use the **cause test** to ensure a complete investigation and sound logic exists; (Precedence, Necessary, Sufficient); the final product, **Event and Causal Factor Tree**, contains all of the underlying causal and/or Contributing Factors supported by evidence.

5. Develop **recommendations to address findings** with the most impact which are clear, verifiable, and achievable; look for cut sets and generate **recommendations in order of effectiveness**.
NASA Human Factors Analysis and Classification System, known as HFACS, and the RCA “Big Sheet” (SHELL-D*) are used to better define events and conditions aspects of mishaps.

This allows the RCA to drive evidence collection well past the "operator error" level to fix systems and processes.