



Learning From NASA Mishaps: What Separates Success From Failure?

**Project Management Challenge 2007
February 7, 2007**

**Faith Chandler
Office of Safety and Mission Assurance**



Discussion Topics

- What is a mishap?
- What is a close call?
- How can they affect your program?
- Anatomy of an accident.
- What can you learn from others past failures that will make you successful?
- What do you do if your program has a mishap?
- How can you prepare your program?



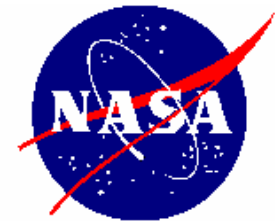
Is the purpose of your program only to serve as a warning to others?



The cause is really obvious...or is it?

Without understanding the cause, how can you fix the problem?

How can you learn from it?



What's A Mishap? What's A Close Call?

NASA Mishap. An unplanned event that results in at least one of the following:

- Injury to non-NASA personnel, caused by NASA operations.
- Damage to public or private property (including foreign property), caused by NASA operations or NASA-funded development or research projects.
- Occupational injury or occupational illness to NASA personnel.
- NASA mission failure before the scheduled completion of the planned primary mission.
- Destruction of, or damage to, NASA property.

New Definition of Close Call. An event in which there is no injury or only minor injury requiring first aid and/or no equipment/property damage or minor equipment/property damage (less than \$1000), but which possesses a potential to cause a mishap.

ALL MISHAPS And CLOSE CALLS ARE INVESTIGATED



How Are Mishaps Classified?

- Classification based on **dollar loss and injury**.
 - (Mission failure based on cost of mission).
- Classification determines type of investigation to be conducted.
- Mishap classification:
 - Type A mishaps – Type D mishaps
 - Close calls

2003



Type A

NOAA N Prime
Processing Mishap
\$223 M

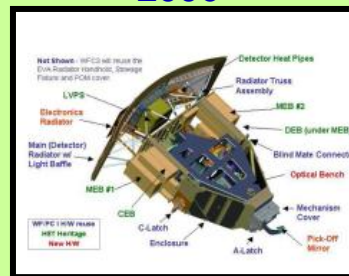
2006



Type B

Remote Manipulator
System Damage by
Bridge Bucket
\$470 K

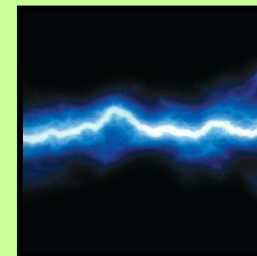
2006



Type C

Hubble WSIPE Lift Sling
Falls on WSIPE Hardware
\$TBD
Between \$25K-\$250K

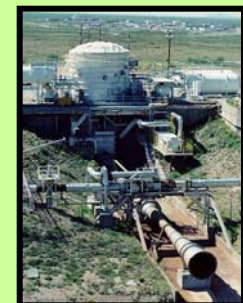
2006



Type D

Hydraulic Pump (HPU-3)
Electrical Arc Between
Pump & Crane Hook
Damage
Less Than \$25K

2005



Close Call

Premature Shutdown of
WSTF Large Altitude
Simulation System &
Blowback on Test Article



How Can Mishaps And Close Calls Affect Your Program?

Mishaps can impact your budget, your schedule, and your mission success!

What Can Go Wrong?

- Equipment can fail
- Software can contain errors
- Humans can make mistakes or deviate from accepted policy and practices

What's The Cost?

- Human life
- One-of-a-kind hardware
- Government equipment & facilities
- Scientific knowledge
- Program cancellation
- Public confidence



40.017 UE Lynch
2005



NASA Mishaps And Close Calls

In 2006, NASA had **715 Mishaps** and **920 Close Calls** reported in the NASA Incident Reporting and Information System (IRIS).

6 Type A mishaps

13 Type B mishaps

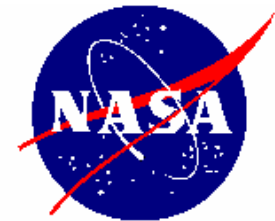
268 Type C mishaps

In the last 10 years (1996-2006), the **direct cost** of mishaps was **more than \$2 Billion**.








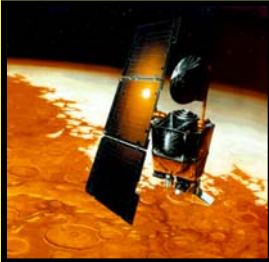






Other Additional Costs Include:

- Worker's compensation
- Training and replacement workers
- Lost productivity
- Schedule delays
- Mishap investigation
- Implementing the Corrective Action Plan (CAP)
- Record keeping (CAP, worker's compensation, mishap, etc)
- Liability

These indirect costs can amount to more, in fact much more, than the direct cost of the injury or property damage.



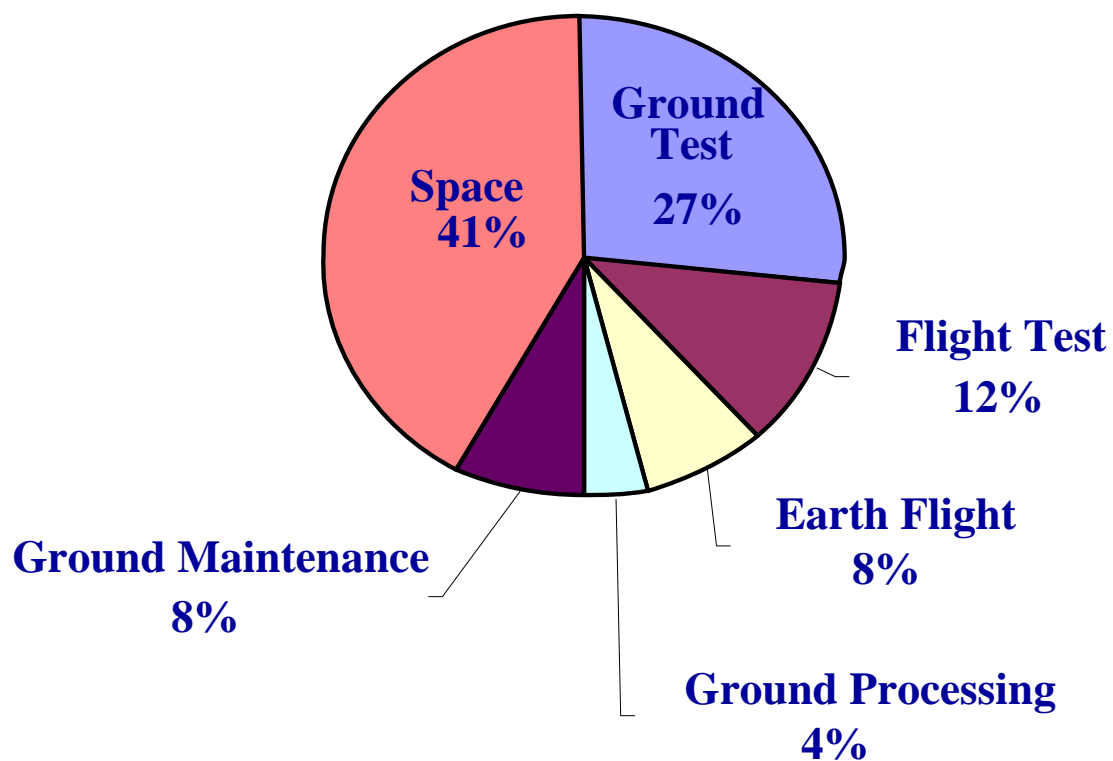
Types Of NASA Mishaps

 <p>CTDs</p>	<p><u>Industrial</u></p>  <p>Cooling Tower Fire</p>  <p>Crane - Pad B</p>	 <p>NOAA N Prime</p>  <p>VAB Foam Fire</p> <p><u>Processing & Test</u></p>	<p><u>Lift Off</u> <u>Test Flight</u></p>  <p>Challenger</p>  <p>Helios</p>	 <p>Mars Climate Orbiter</p>  <p>DART</p> <p><u>In Space</u></p>	<p><u>Landing</u></p>  <p>Columbia</p>  <p>Genesis</p>
<p><u>Individual</u></p>  <p>Slips, Trips, & Falls</p>  <p>Insect & Animal Bites</p>  <p>Automobile</p>					



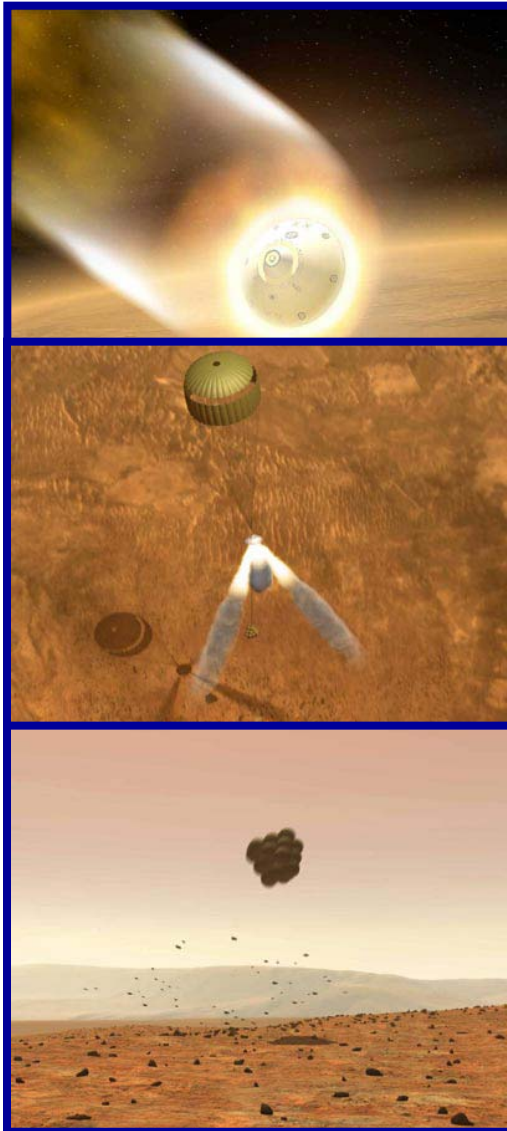
Type Of Activity Where Mishaps Occurred

Percentage of Type A Mishaps
Occurring During Each Type of Activity
1996-2005





Close Calls And Mishaps



Mars Exploration Rovers

Even programs with great success have significant failures and close calls!

- Cancellation of one rover due to concerns about ability to be ready safely for launch.
- Air bag failure months before launch.
- Parachute failure months before launch.
- Potential cable cutter shorting days before launch.
- Pyrotechnic firing software concern one day before Mars arrival.

Why Do Some Programs Have Close Calls And Others Have Mishaps?



Controls and Barriers Fail or Are Non-Existent



VAB CLOSE CALL 2006

2 Men Fall From Ladder
Sustain Slight Injuries

Control: Fall Protection Used



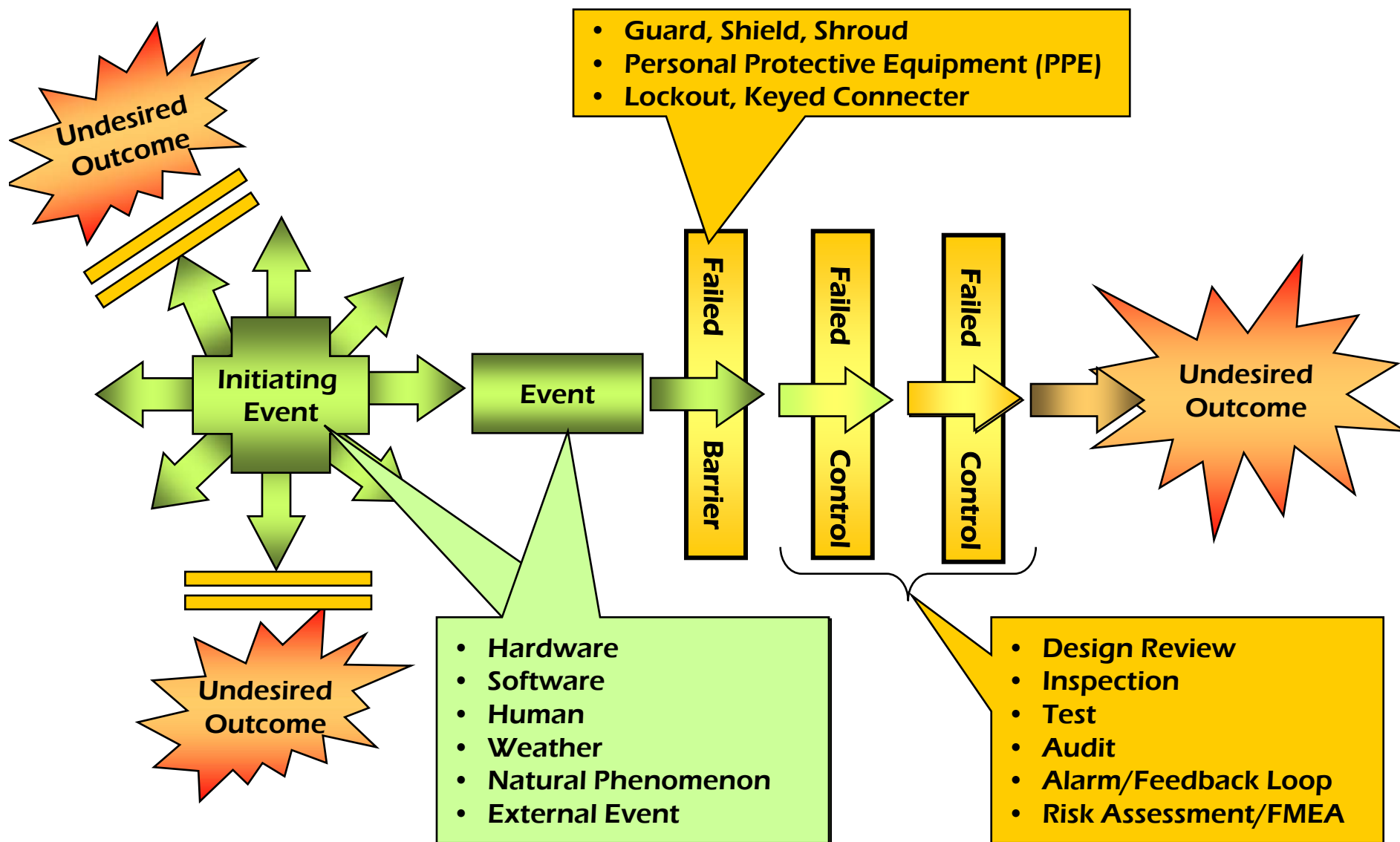
Bldg. M6-794 TYPE A MISHAP 2006

1 Man Falls From Roof
Fatality

Control Failed: Fall Protection NOT Used



Anatomy Of An Accident



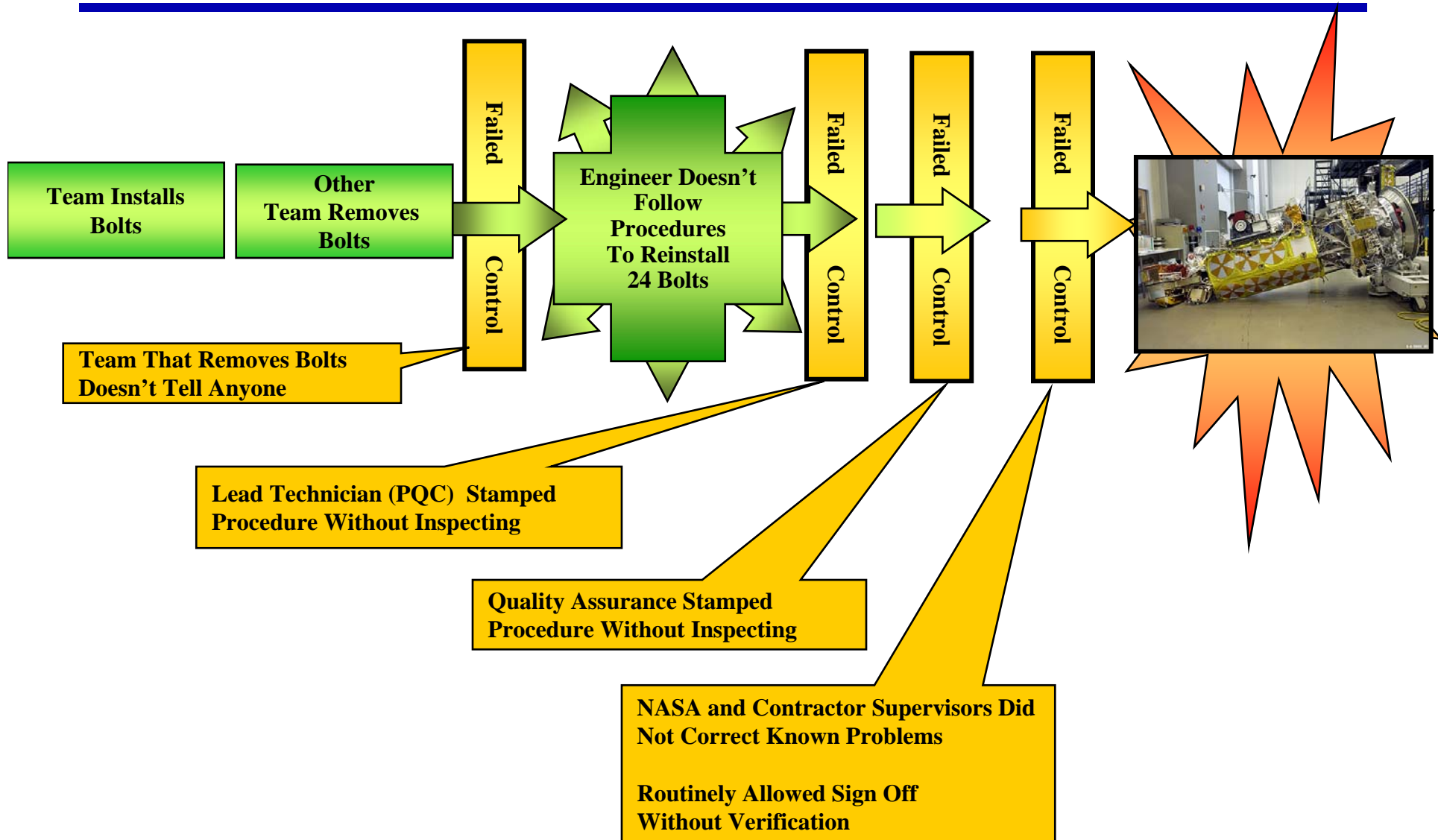


How To Make Sure Your Program Doesn't Have A Major Mishap

- It is **Not** enough to have layers of defenses... Nearly every program at NASA has them.
 - Reviews
 - Inspections
 - Tests
 - Audits
 - Alarms and means to mitigate
- What separates the successful programs from those that have mishaps... **These defenses work**
- **How can you detect failing or non-existent defenses?**
 - Perform Root Cause Analysis (RCA) on problems and close calls.
 - Identify systemic problems in your program.
 - Fix failures in defenses early ... before they cause a mishap.



NOAA N Prime's Weak Defenses





What Can Your Program Learn From NOAA N Prime?

- Communicate all changes on the floor to all technicians and supervisors.
 - Is this really working in your program now?
- Do not back stamp procedures
 - Are your technicians doing this now?
 - This has been a factor in many mishaps!
- If an audit or an investigation identifies a problem, or a non-conformance, fix it!
 - This has been a factor in previous mishaps



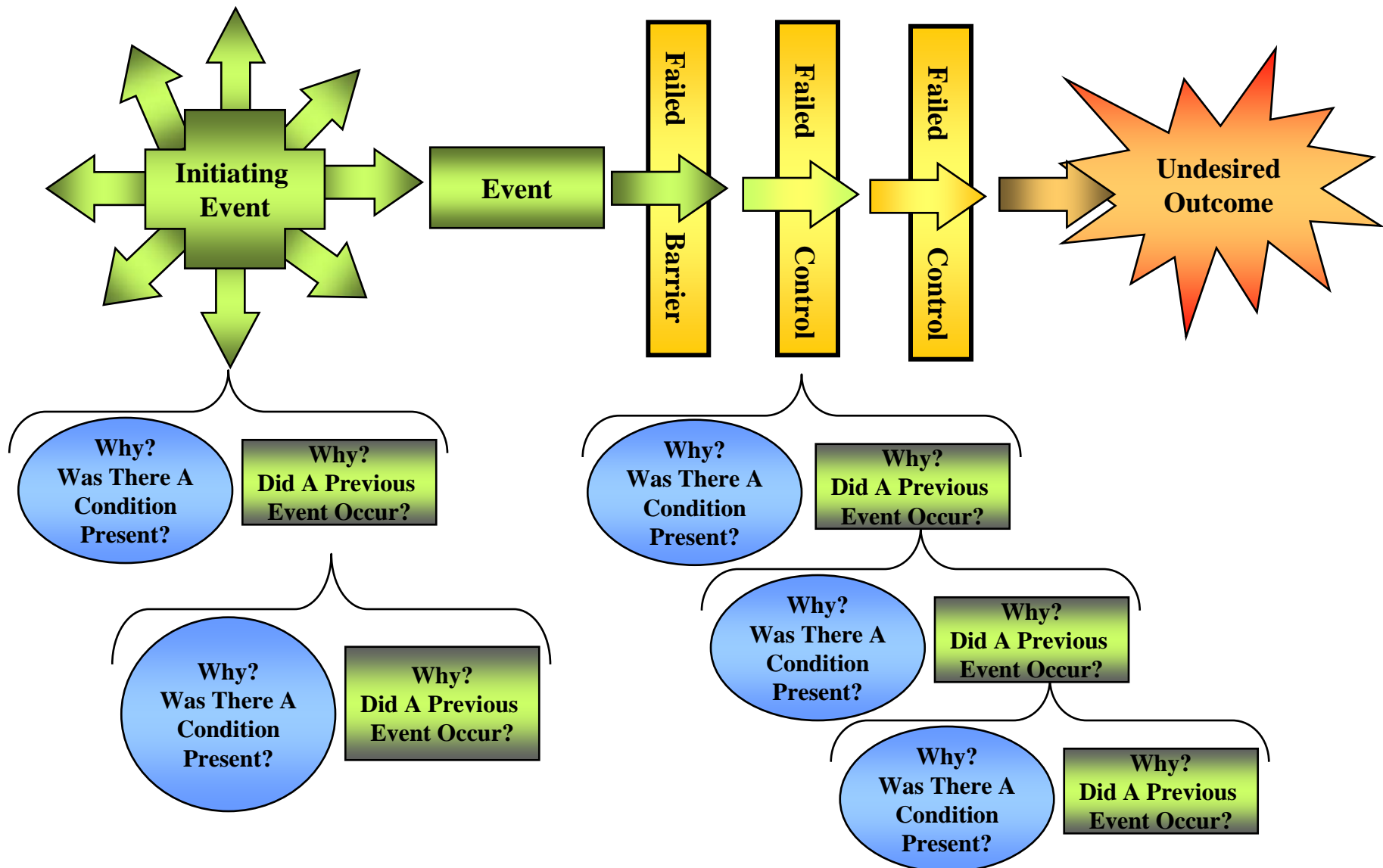
Understanding The Mishap

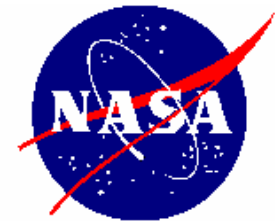
- Initiating events happen.
- Defenses (Controls and Barriers) fail or do not exist.

But why?



Anatomy of an Accident – Asking Why

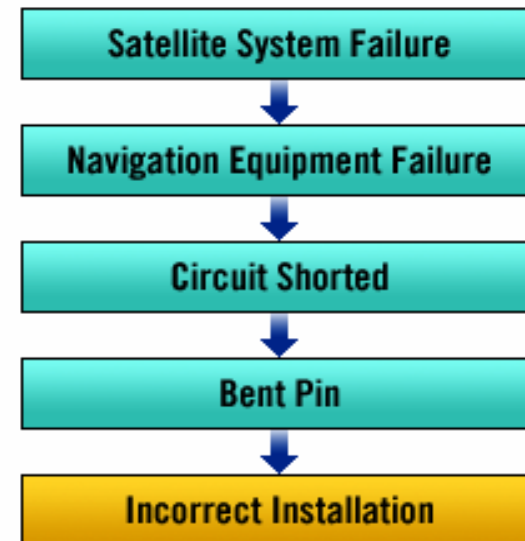




Investigating Accidents

Often we:

- Identify the part or individual that failed.
- Identify the type of failure.
- Identify the immediate cause of the failure.
- Stop the analysis.



Is this the root cause?

☐ No ☐ Yes

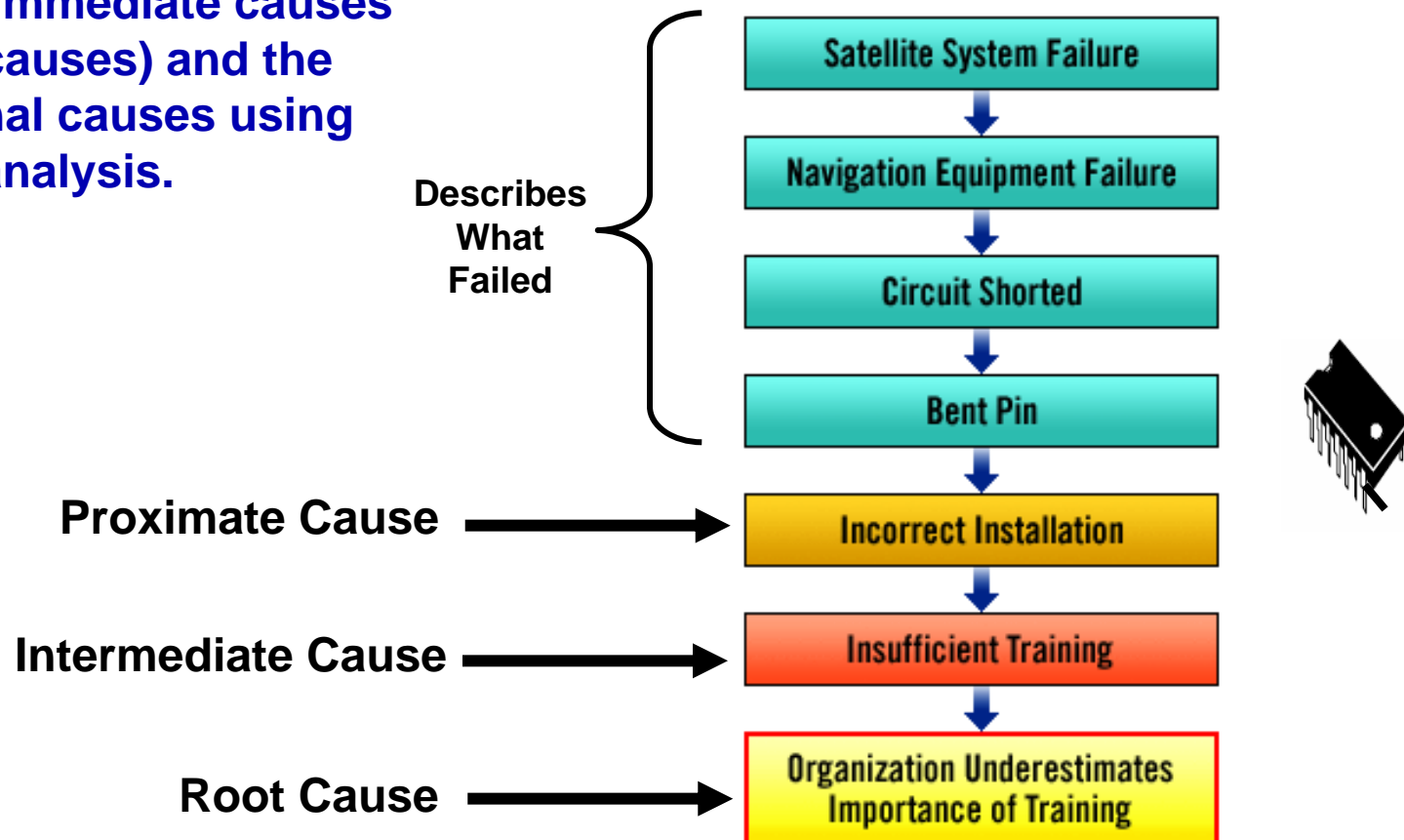
Problem with this approach:

The underlying causes may continue to produce similar problems or mishaps in the same or related areas.



Root Cause Analysis

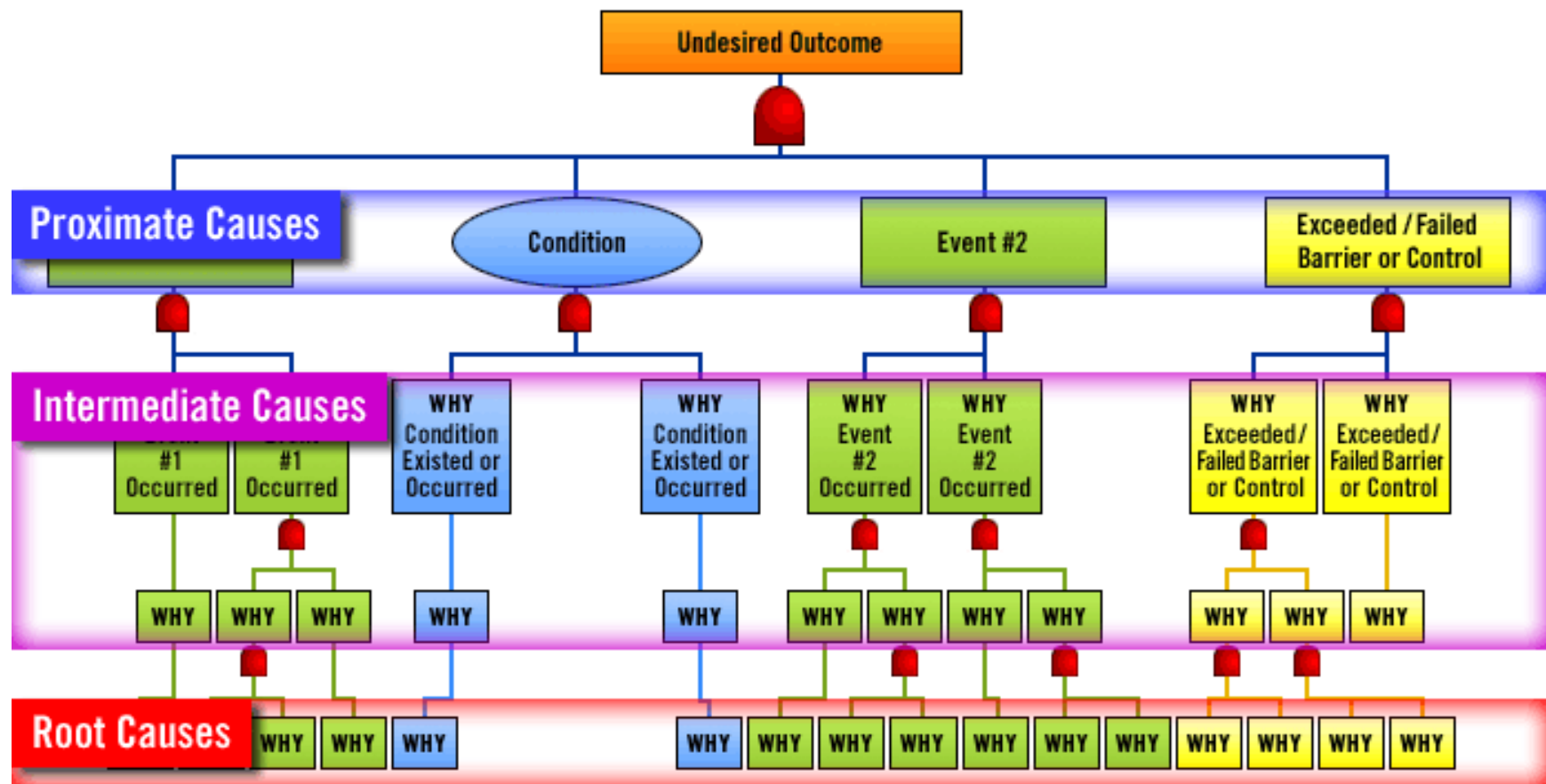
Identify the immediate causes (proximate causes) and the organizational causes using root cause analysis.





Root Cause Analysis

Event and Causal Factor Tree: Shows all the things that did occur.





Anhydrous Ammonia



Will Your Program Implement The Lessons Learned?



- Genesis spacecraft launch, August 8, 2001
- Collect solar wind samples for two years
- Returned to Earth on September 8, 2004
- Most science was recovered



Parachute failed to deploy

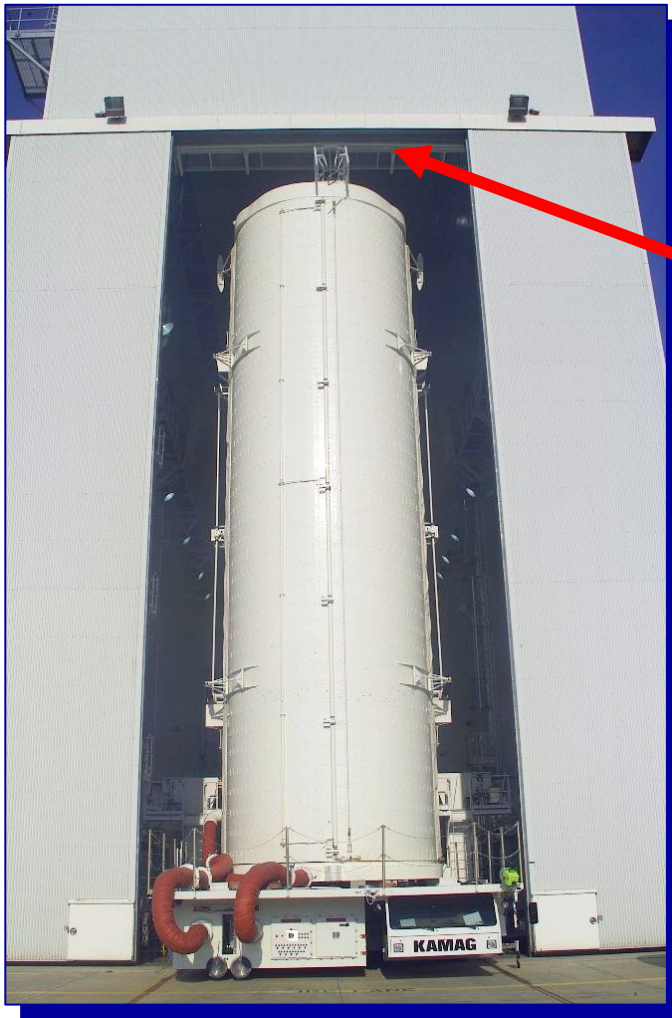
Some of the Causes

- Design error - G-Switch inverted (Inappropriate confidence in heritage design)
- Drawing incorrect
- Drawing error not detected:
 - Reviews not in depth
 - Testing deleted/modified

Will Your Program Implement The Lessons Learned?



Canister Ladder Contacted Canister Rotation Facility Door – 2001



- Configuration change – added ladder
- Didn't review or analyze change.
- No documentation of clearance height.
- Procedures did not require a check of canister stack height and facility clearance prior to move.
- No detection during move.



Will Your Program Implement The Lessons Learned?



- Helios Test Flight, June 23, 2003.
- High dynamic pressure reached by the aircraft during an unstable pitch oscillation leading to failure of the vehicle's secondary structure
- *"Helios suffered from incorrect assessment of risk as the result of inaccurate information provided by the analysis methods and schedule pressures and fiscal constraints resulting from budgetary contraction, constrained test windows and a terminating program. Though the pressures and constraints were not considered unusual, it did have some unquantifiable influence on the decision process."* (MIB report)

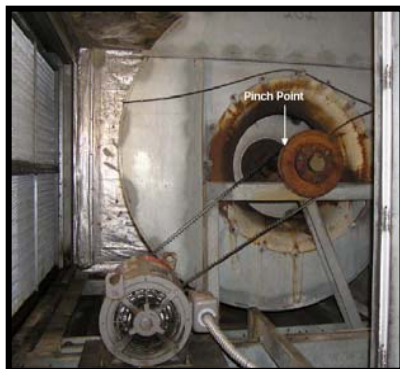
Summary of Causes of Mishap

- Configuration change – 2 fuel cells to 3 fuel cells
- **Reviews did not identify problem** - change in the vehicle's weight and balance that stability
- Lack of adequate analysis methods
- **Inaccurate risk assessment** of the effects of configuration changes
- **Didn't do incremental testing after change.**
- This led to an inappropriate decision to fly an aircraft configuration highly sensitive to disturbances.

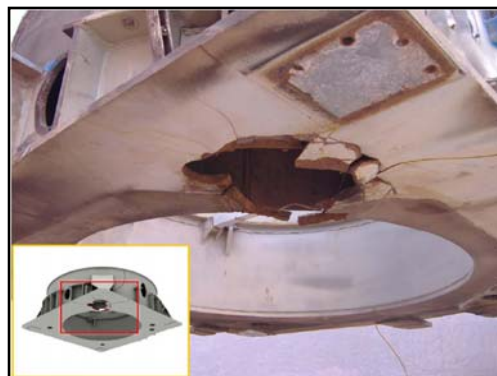




Can You See A Pattern?



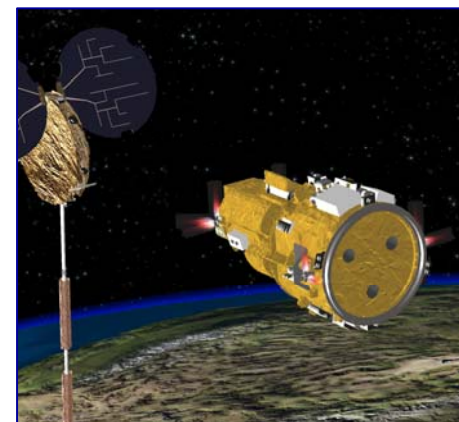
Type B
Finger Amputation
In Pulley



SLC-2 VAFB
2006



Astro E2 – Suzaku
2005

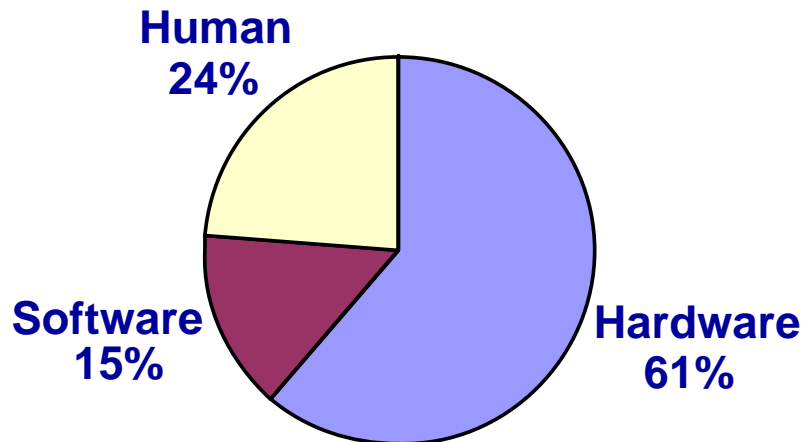


DART 2005



What Causes Mishaps?

Proximate Cause of Type A Mishaps 1996-2005



NASA

- **57% of Type A mishaps caused by human error (1996-2005)**

*Does not include auto accidents or death by natural causes

- **78% of the Shuttle ground-support operations incidents resulted from human error (Perry, 1993).**

Outside NASA

- **75% of all US military aircraft losses involve sensory or cognitive errors**
(Air Force Safety Center, 2003).

- **83 % of 23,338 accidents involving boilers and pressure vessels were a direct result of human oversight or lack of knowledge**

(National Board of Boiler and Pressure Vessel Inspectors, 2005).

- **41% of mishaps at petrochemical plants were caused by human error**

(R.E. Butikofer, 1986).

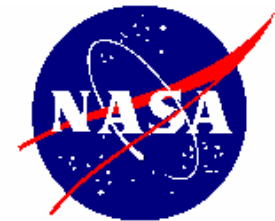


Lessons Learned: What Causes Mishaps?

Unsafe acts occur in all programs and phases of the system life cycle.

- Specification development/planning
 - Conceptual design
 - Product design
 - Fabrication/production
 - Operational service
 - Product decommissioning
-
- 70-90% of safety-related decisions in engineering projects are made during early concept development.
 - Decisions made during the design process account for the greatest effect on cost of a product.

- Design process errors are the root cause of many failures.
- Human performance during operations & maintenance is also a major contributor to system risk.



Type A - Payload Mishaps



HESSI (2000)

High Energy Solar Spectroscopic Imager

Subjected to a series of vibration tests as part of its flight certification program...caused significant structural damage.

- Misaligned shaker table
- No validation test of shaker table
- HESSI project not aware of risk posed by test
- Sine-burst frequency not in the test plan
- Written procedure did not have critical steps

SOHO (1998)

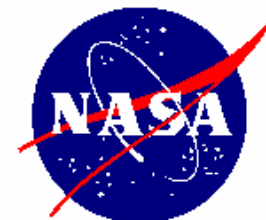
Solar Heliospheric Observatory



- Made changes to software and procedures
- Failed to perform risk analysis of modified procedure set
- Ground errors led to the major loss of attitude (Omission in the modified predefined command)
- Failure to communicate procedure change
- Incorrect diagnosis



NASA

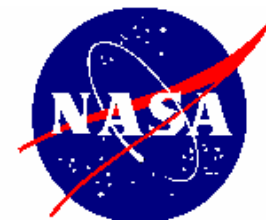


Causes Of Mishaps – Inside NASA

Design
<ul style="list-style-type: none">• Logic design error existed - Design errors in the circuitry were not identified
<ul style="list-style-type: none">• Drawing incorrect
<ul style="list-style-type: none">• System drawings were incorrect because they were not updated when system was moved from its original location to the Center
<ul style="list-style-type: none">• System labels were incorrect
<ul style="list-style-type: none">• System did not have sensors to detect failure
<ul style="list-style-type: none">• Configuration changes driven by programmatic and technological constraints... reduced design robustness and margins of safety

Reviews
<ul style="list-style-type: none">• Design was not peer reviewed
<ul style="list-style-type: none">• Systems reviews were not conducted
<ul style="list-style-type: none">• Technical reviews failed to detect error in design
<ul style="list-style-type: none">• Red-Team Reviews failed to identify design errors

Tests
<ul style="list-style-type: none">• Testing only for correction functional behavior ... not for anomalous behavior, especially during initial turn-on and power on reset conditions
<ul style="list-style-type: none">• There was no end-to-end test.
<ul style="list-style-type: none">• Test procedure did not have a step to verify that all critical steps were performed
<ul style="list-style-type: none">• Lacked a facility validation test
<ul style="list-style-type: none">• Failed to test as fly...fly as you test
<ul style="list-style-type: none">• Tests were cut because funding was cut



Causes Of Mishaps – Inside NASA

Operations

- Team error in analysis due to lack of system knowledge. This contributed to the team's lack of understanding of essential spacecraft design
- **Incorrect diagnosis** of problem because the team lacked information about changes in the procedures
- Emergency step/correction maneuver was not performed

Communication

- **Inadequate communication between shifts**
- Inadequate communications between project elements

Paperwork

- Lacked documentation on system characteristics
- Processing paperwork and discrepancy disposition paperwork were ambiguous
- Electronic paperwork system can be edited with no traceability (Info was changed and no record of the change was recorded)
- Written procedures generally did not have full coverage of the pretest setup and post-test teardown phases of the process
- **Did not follow procedures** (led to fatality)
- Procedure did not have mandatory steps



Causes Of Mishaps – Inside NASA

Supervision

- **“Failure to correct known problems”** was a supervisory failure to correct similar known problems (Hardware)
- **Supervisory Violation”** was committed by repeatedly **waiving required presence of quality assurance and safety** and bypassing Government Mandatory Inspection Points
- Lacked “organizational processes” to effectively monitor, verify, and audit the performance and effectiveness of the processes and activities

Staffing

- Inadequate operation’s team staffing

Risk Assessment & Risk Mgmt

- Did not consider the worst-case effect. Lacked systematic analyses of “what could go wrong”
- The perception that operations were routine resulted in inadequate attention to risk mitigation
- The project was **not fully aware of the risks** associated with the test
- Lack of adequate analysis methods led to an inaccurate risk assessment of the effects of configuration changes



What happens when a mishap or close call occurs?





Immediate Notification Process

Within 1 Hour

- Center Safety Office- **Notify Headquarters by Phone** = for Type A, Type B, high visibility mishap, or high visibility close call. This includes reporting a human test subject injury/fatality)
 - Duty 202.358.0006
 - Non-duty 866.230.6272
- Chief, Safety and Mission Assurance – **Notify Administrator** and senior staff (phone and/or mishap lists email)
- Center's Chief of Aircraft Operations- **Notify National Transportation Safety Board** (NTSB) if applicable

Within 8 Hours

- **Notify OSHA** (if applicable)
- Applicable:
Up to 30 days after mishap when:
- Death of federal employee
 - Hospitalization 3 or more if 1 is a Federal Employee

Within 24 Hours

- Center Safety Office-**Notify Headquarters electronically with additional details**
- Center Safety Office- **Record the occurrence of ALL mishaps & close calls** in Incident Reporting Information System (IRIS)
 - Center Director- **Notify Administrator** by phone when the following occur:
 - Type A
 - Type B
 - Type C (Lost-time injury only)
 - Onsite non-occupational fatality (e.g., heart attack)
 - Fatalities and serious illness off the job (civil servant & contractor)



Mishap Investigation Notional Timeline





Two Types of Mishap Investigations

- Safety Mishap Investigation
(Per NPR 8621.1: NASA Procedural Requirements for Mishap Reporting, Investigating and Recordkeeping)
 - Describes policy to report, investigate, and document mishaps, close calls, and previously unidentified serious workplace hazards to prevent recurrence of similar accidents.
- Collateral Mishap Investigation
(Procedures & requirements being developed by the Office of the General Counsel).
 - If it is reasonably suspected that a mishap resulted from criminal activity.
 - If the Agency wants to access accountability (e.g., determine negligence).



Why Should You Investigate Close Calls?

- Investigations can identify systemic problems
- Close calls can help you a lot...**They tell you where your problems are.**
- Close calls give you the opportunity to influence your program/project along the way.

**Requiring your teams to
report and investigate close calls.**



Preparing For Mishaps



Who's Missing
Hardware?



July 2006
LaRC Wind Tunnel



Preparing For Mishaps

- **Anticipate the failures**
- **Write failure report first... if failed why would we have failed? Generate your plans accordingly.**
- **A good designer thinks about how someone will use a tool, piece equipment, or procedure (etc.) and how will it be mis-used. Think about it early on! Prepare for the mis-use.**
- **For critical failures have a Mishap Preparedness and Contingency Plan that covers:**
 - ✓ **Manufacturing Mishaps**
 - ✓ **Processing Mishaps**
 - ✓ **Test Mishap**
 - ✓ **Transportation Mishap**
 - ✓ **Flight Mishaps**
 - ✓ **Operations Mishaps**

What does your Mishap Preparedness and Contingency Plan look like? Successful programs have complete plans.



Preparing For Mishaps

- Center Mishap Preparedness and Contingency Plan Contents
 - Local close call and mishap reporting & investigating procedures
 - Center-specific emergency response
 - Procedures to appoint an Interim Response Team
 - Location of space for impounded objects
 - Mishap process to establish investigating authority and process report (Type C mishaps, Type D mishaps, and close calls)
- Program Mishap Preparedness and Contingency Plan Contents
 - Specific procedures for program emergency response and investigating (e.g., safing procedures, toxic commodities, ...)
 - Names chair and ex-officio for a Type A board.
 - Procedures to impound data, records, etc... for off-site mishaps
 - Lists national, state, and local organizations and agencies which are most likely to take part in debris collection
 - Lists MOUs with international partners and agencies that may support investigation



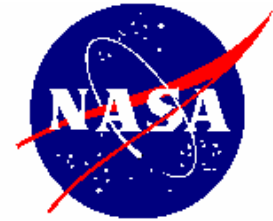
For More Information

- NASA PBMA Mishap Investigation Website
(<https://secureworkgroups.grc.nasa.gov/mi>)
 - Includes:
 - Requirements
 - Guides and handbooks
 - Template
 - Tools and methods
 - Hard copies of classroom training
 - Mishap reports
 - Lessons learned
 - Conference presentations
- HQ Office of Safety & Mission Assurance
 - Faith.T.Chandler@nasa.gov
 - 202-358-0411



Conclusion

- “Lots of times we’re lucky or prepared and we dodge the bullet...”
- But sometimes we endure very public failures, loss of life and significant loss of property...
- In every case, we work to prevent failures and ensure success...
- And when failures occur, we try to learn from them.”
(Tattini... Mars Exploration Rover)
- To be successful, we must report and investigate our failures and close calls, identify the underlying root causes, and generate solutions that prevent these systemic problems from creating more failures in our program and in others.



BACK-UP SLIDES



NASA Mishap And Close Call Classification Levels

Classification Level	Property Damage	Injury
Type A	<p>Total direct cost of mission failure and property damage is \$1,000,000 or more,</p> <p><i>or</i></p> <p>Crewed aircraft hull loss has occurred,</p> <p><i>or</i></p> <p>Occurrence of an unexpected aircraft departure from controlled flight (except high performance jet/test aircraft such as F-15, F-16, F/A-18, T-38, and T-34, when engaged in flight test activities).</p>	<p>Occupational injury and/or illness that resulted in:</p> <p>A fatality,</p> <p><i>or</i></p> <p>A permanent total disability,</p> <p><i>or</i></p> <p>The hospitalization for inpatient care of 3 or more people within 30 workdays of the mishap.</p>
Type B	<p>Total direct cost of mission failure and property damage of at least \$250,000 but less than \$1,000,000.</p>	<p>Occupational injury and/or illness has resulted in permanent partial disability.</p> <p><i>or</i></p> <p>The hospitalization for inpatient care of 1-2 people within 30 workdays of the mishap.</p>
Type C	<p>Total direct cost of mission failure and property damage of at least \$25,000 but less than \$250,000.</p>	<p>Nonfatal occupational injury or illness that caused any workdays away from work, restricted duty, or transfer to another job beyond the workday or shift on which it occurred.</p>
Type D	<p>Total direct cost of mission failure and property damage of at least \$1,000 but less than \$25,000.</p>	<p>Any nonfatal OSHA recordable occupational injury and/or illness that does not meet the definition of a Type C mishap.</p>
Close Call	<p>An event in which there is no equipment/property damage or minor equipment/property damage (less than \$1000), but which possesses the potential to cause a mishap.</p>	<p>An event in which there is no injury or only minor injury requiring first aid, but which possesses a potential to cause a mishap.</p>



Definitions of RCA & Related Terms

Cause (Causal Factor)	An event or condition that results in an effect. Anything that shapes or influences the outcome.
Proximate Cause(s)	The event(s) that occurred, including any condition(s) that existed immediately before the undesired outcome, directly resulted in its occurrence and, if eliminated or modified, would have prevented the undesired outcome. Also known as the <u>direct cause(s)</u> .
Root Cause(s)	One of multiple factors (events, conditions or organizational factors) that contributed to or created the proximate cause and subsequent undesired outcome and, if eliminated, or modified would have prevented the undesired outcome. Typically multiple root causes contribute to an undesired outcome.
Root Cause Analysis (RCA)	A structured evaluation method that identifies the root causes for an undesired outcome and the actions adequate to prevent recurrence. Root cause analysis should continue until organizational factors have been identified, or until data are exhausted.
Event	A real-time occurrence describing one discrete action, typically an error, failure, or malfunction. Examples: pipe broke, power lost, lightning struck, person opened valve, etc...
Condition	Any as-found state, whether or not resulting from an event, that may have safety, health, quality, security, operational, or environmental implications.
Organizational Factors	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. Examples: resource management (budget, staff, training); policy (content, implementation, verification); and management decisions.
Contributing Factor	An event or condition that may have contributed to the occurrence of an undesired outcome but, if eliminated or modified, would not by itself have prevented the occurrence.
Barrier	A physical device or an administrative control used to reduce risk of the undesired outcome to an acceptable level. Barriers can provide physical intervention (e.g., a guardrail) or procedural separation in time and space (e.g., lock-out-tag-out procedure).