Eighth Annual SSRM Symposium

Risk Mitigation for Managing On-Orbit Anomalies

Jim La
NASA/GSFC/Code 302
Institution Support Center

April 6-8, 2010

Background

- Risk is inherent in all space missions. Effective identification & management of risk are critical responsibilities of project management & often determine whether a mission will be successful

- Risk Management is the focused unrelenting effort to confront uncertainty and bring it into adjustment with technical, safety, cost, and schedule

- Risk is also the probability that an unfavorable result will occur & severity of its consequences. It can take various forms:
  - Technical
  - Programmatic or Political
  - Mission Operations
  - Schedule
  - Cost

Agenda

- Issues associated with Mission Operations
- Dealing with the unknown
- Searching for root causes
- Developing recovery options
- MOA for Mission Success

Risk Associated with Mission Ops

- Program maintenance & operation must recognize that Mission Operations is not just "operations" in the usual meaning
- Most satellites reach "operational" status after on-orbit verification tests, significant reduction in the workforce to meet Zero Base Review requirements
- Safety & Mission Assurance function reduces the risk of human single point failures
- Ensure common practices and processes are consistently applied throughout the Agency
- Ensure lessons learned from investigations are captured and shared among the projects and missions
- Insure adequate time spent to investigate and resolve anomalies

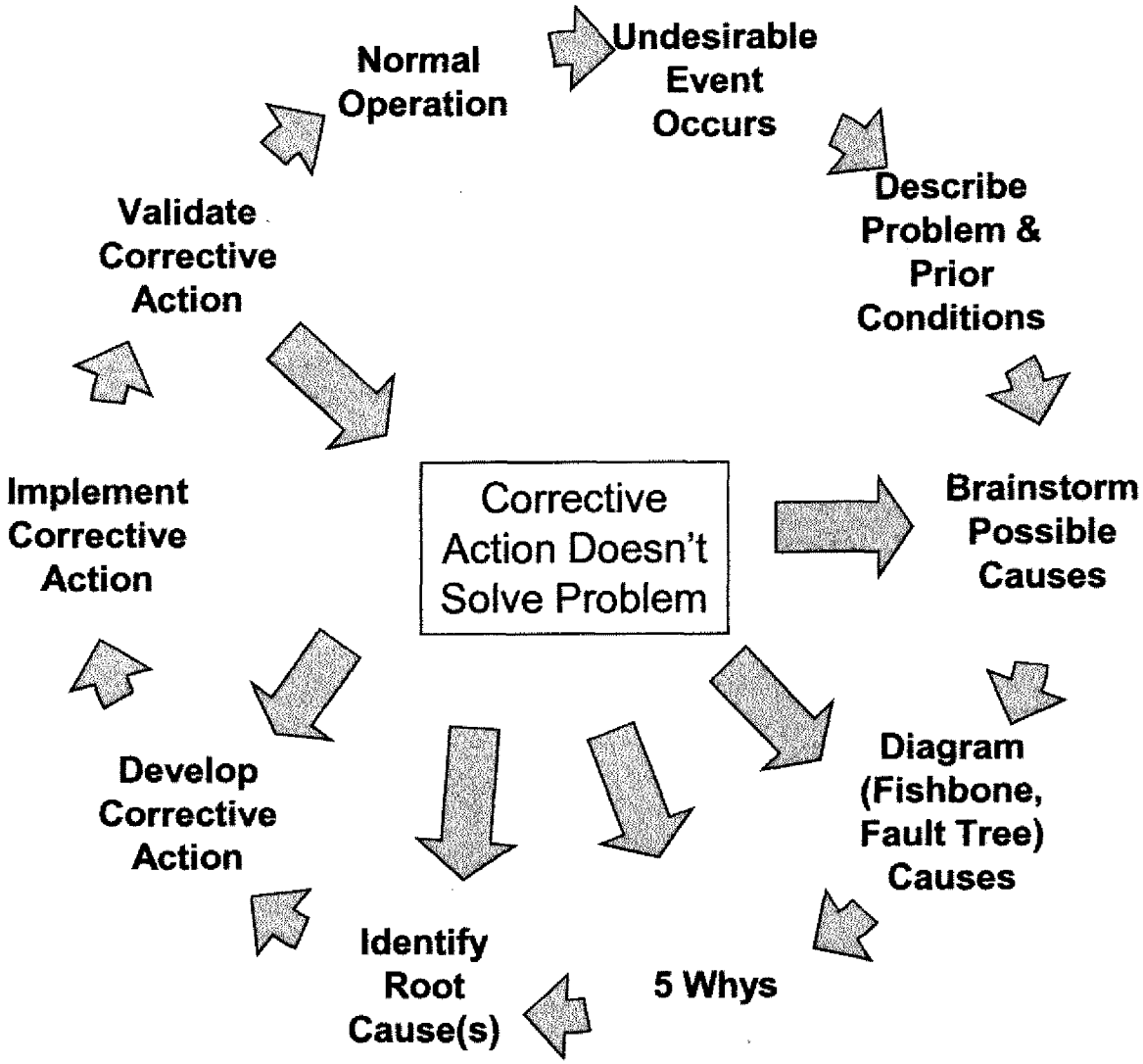
Why is Mission Ops Assurance important?

- Improve Operational Reliability of Spacecraft During Mission Operations.
- Ensure Program & Mission Objectives, Spacecraft Design & Capabilities, and Flight Operations Planning & Implementation are Compatible and Consistent.
- Facilitate Integration of the Mission Assurance Function Into the Project so that All Team Members Share Responsibility for Program & Mission Success.
- Assure the Design, Implementation, Integration, Validation & Execution of Operations Processes are Sufficient to Successfully Accomplish Program & Mission Objectives.
- Provide the Project Management Team and Institutional Management Visibility Into Mission Operations Issues, Concerns and Recommendations, as Appropriate.
- Perform Independent Risk Assessments of Operational Activities Particularly for Upcoming Critical Events
- Provide Direct Transfer of Knowledge and Experience to Existing and Future Flight Projects.

Manage Risk with Known Issues

- Participate in mission ops level risk reviews with a focus on compliance to the current policy requirements for risk management.
  - This may result in the following:
    - Use of Failure Modes and Effects Analysis (FMEA)- procedure, by which each potential failure mode of each element of a system is analyzed to determine the effects of the failure mode on the system and to classify each potential failure mode of according to the severity of the effects.
    - Use of Fault Tree Analysis (FTA)- a qualitative technique to uncover credible ways that a top event (undesired) can occur. The results of the FTA are documented in a fault tree, which is a graphical representation of the combination of the faults that will result in the occurrence of an undesired to event.
- Maintain list of Mission Ops high priority (top 'n') risks.
  - Risk list is the listing of all identified Mission Ops risk in priority order from highest to lowest risk, together with the information that is needed to manage each risk and document its evolution over the course of the project.

Manage Undesirable Events Risks



Closed Loop Fault Analysis & Corrective Action

- **Event occurs**
  - Document the condition and the activities that lead up to the event
- **Brainstorming**
  - What do we Know?
- **Develop and Event or process Causal factor flow diagram**
  - Build an event sequence / causal factor sequence diagram
- **Develop fish bone *or* Develop a Root cause Tree or Map**
- **Eliminate not-possible causes**
  - determine most probable cause
- **Develop recovery options**
- **Build an event sequence diagram for recovery plan**
  - Identify success criteria for each event
- **Validate, Implement and verify plan**

Describe Problem and Prior Conditions

- Finding the root cause by first collecting all appropriate data that lead up to the event and to date
  - Each team member document what they know *(with out input from others)*
  - What events occurred
    - What did they do
    - What did they see
      - Facts first
      - Them assumptions
    - Look back to a point in time sound data support normal operations
      - May need to go back farther based on event/failure
    - Including commands sent
    - Files loaded
    - Procedures executed
    - Environment activities, (ground and space)
    - Change in mission profile
    - Personal, changes, etc.
  - What is the Last known state of the system
    - All elements not just the failed element
- This will support building event sequence and timeline

Brainstorming for Root Cause - Fish Bone Diagram

- **Fish bone**
  - Develop fishbone diagram if greater detail is need
  - Aids in driving out possible failure factors
    - Develops a comprehensive picture of potential causes
    - bounds the condition
  - Start with Failure condition as the effect
  - *Use Data, SW, HW, human error, environment* as possible errors (bones)
    - **Ask How this bone could have contributed**
  - Functional Fault tree, Event driven and functional block diagram will aid in this process

Example -

- Condition
  - Mission Operations Center (MOC) notification

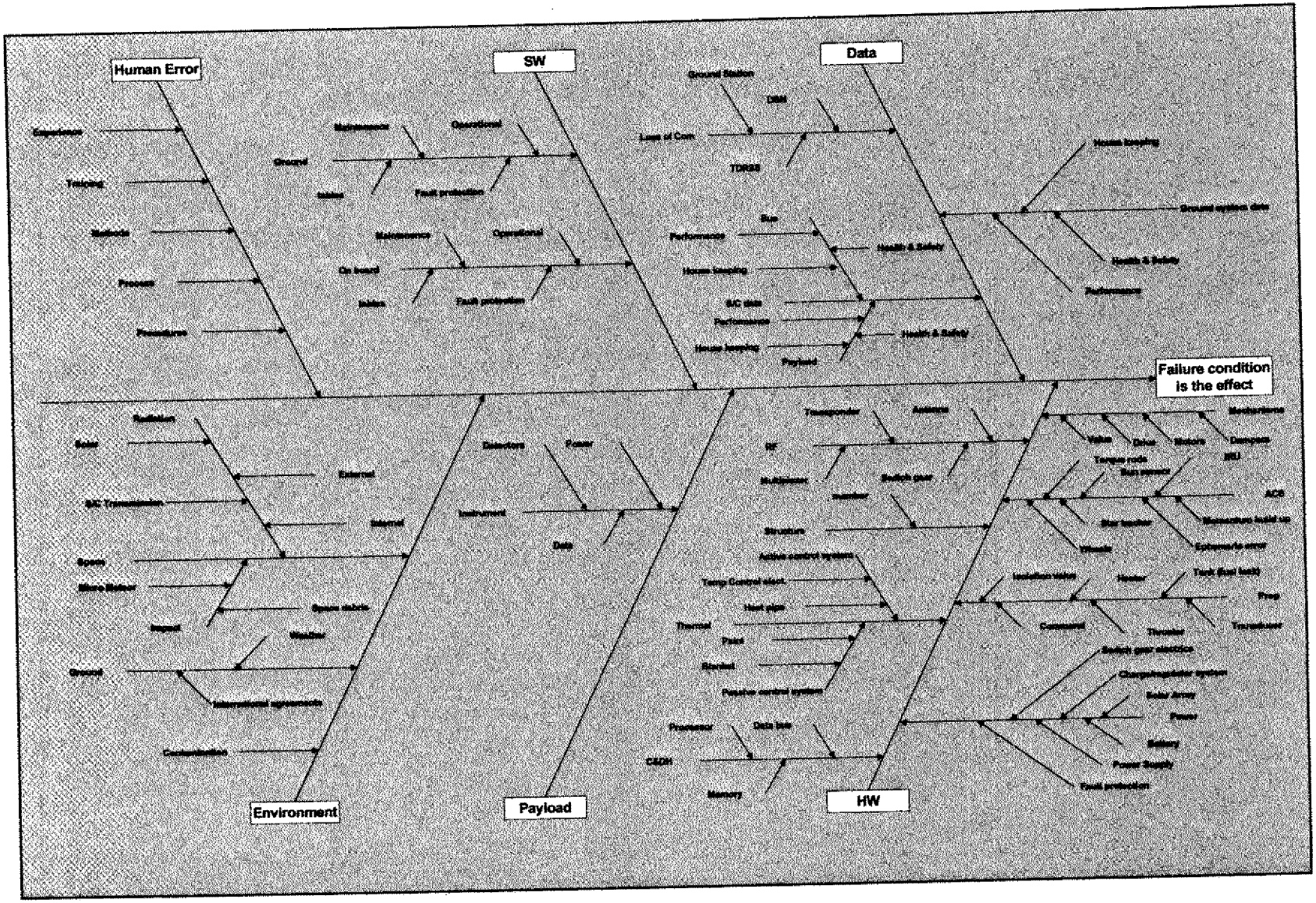
    S/C transitioned into sun/mag-reference pointing mode at the end of a slew

  - Next bad quaternions generated due to star ID problems

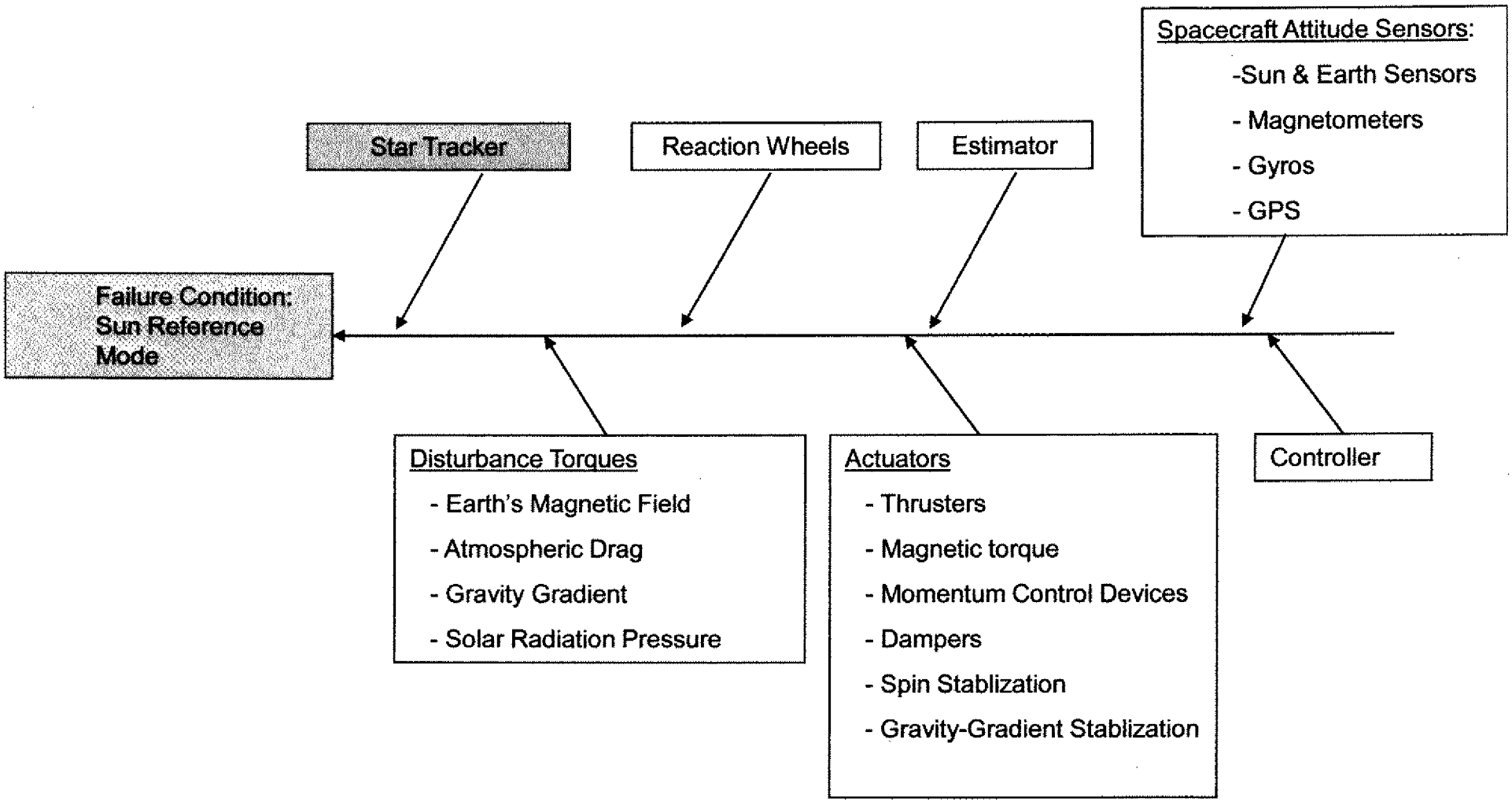
  - S/C not achieving and/or holding required attitude

Now lets talk about the tools we used to find this

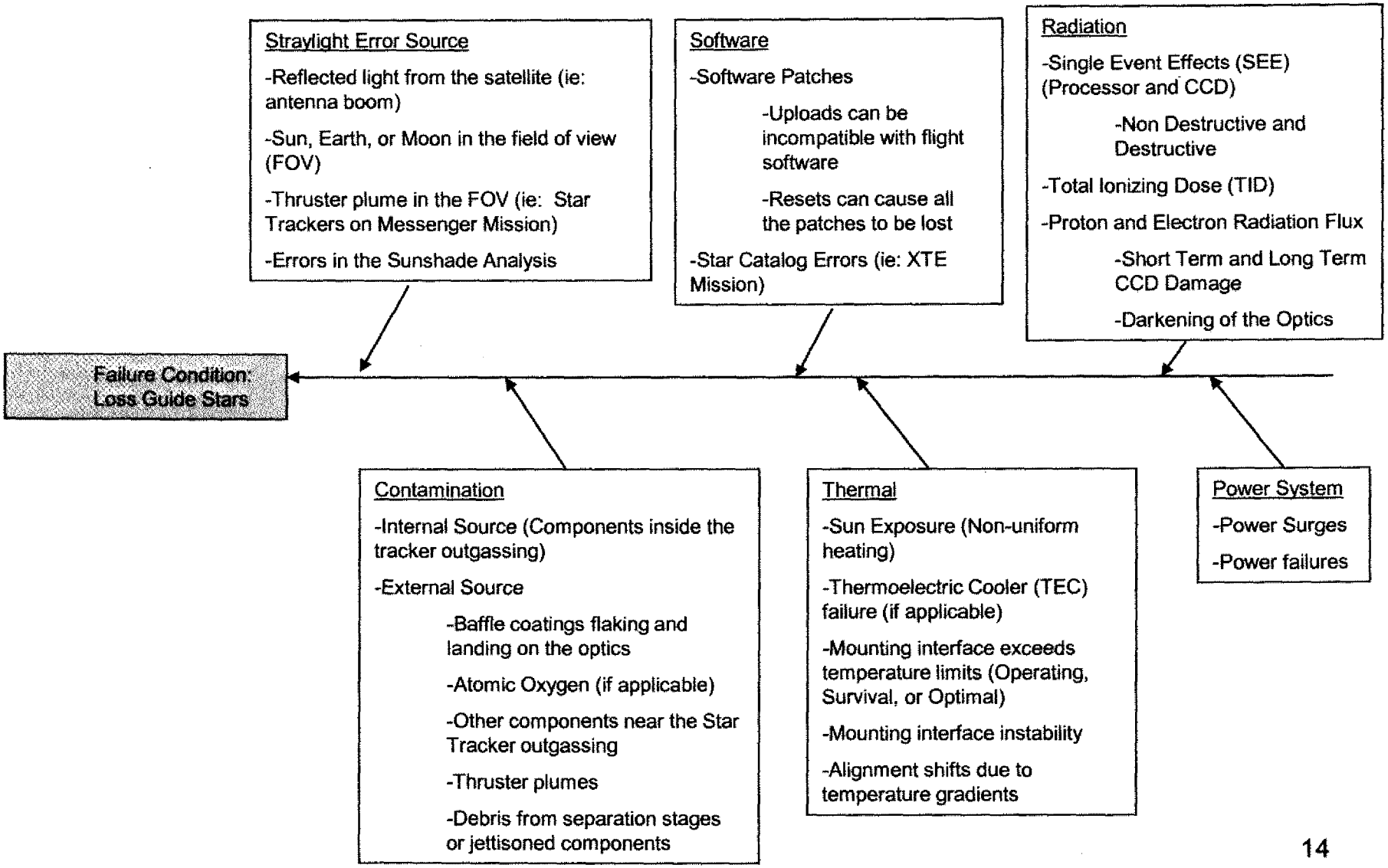
Example Fish Bone Diagram
Flight & Ground System



Attitude Control System



Star Tracker



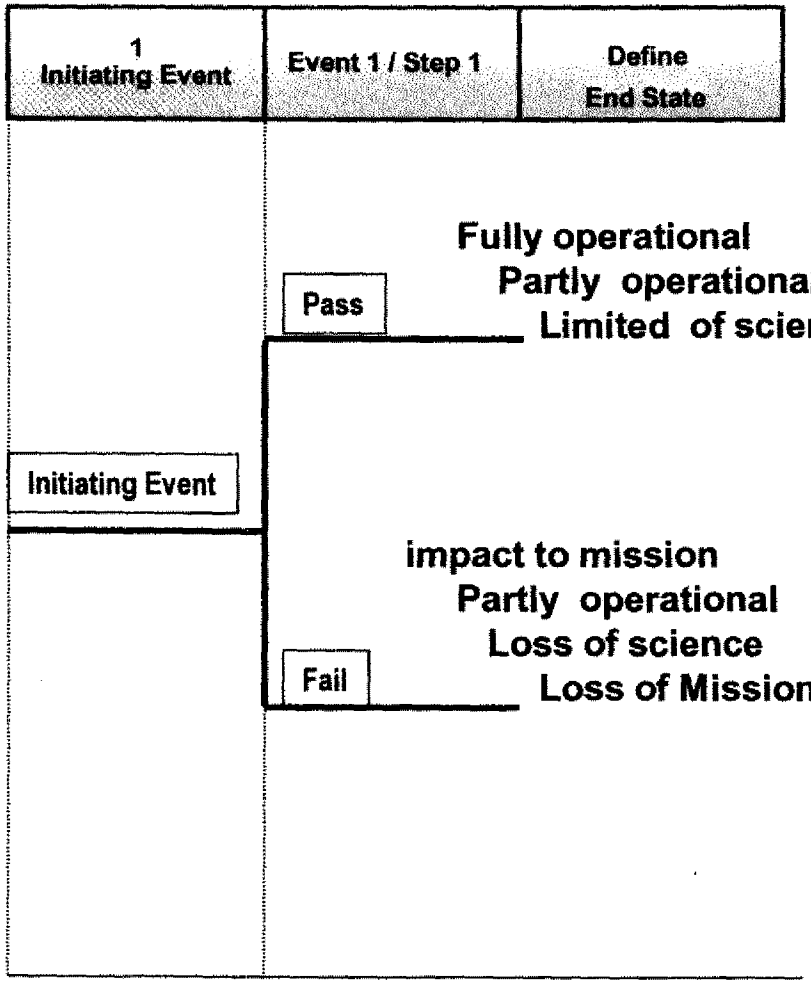
Develop an Event & Process Flow Diagram

Additional Tools for Root Cause Analysis if more detail is needed

- **Build an event sequence with a time lime for normal ops**
  - Repeat the process with the events that occurred
  - The undesired event is the starting point for the next step

- **Develop a Root causal Tree or Map**
  - Populate a causal factor diagram
  - Place undesired event at top of tree
  - Ask What are the events, conditions and exceeded/failed controls or barrier that occurred leading up to the event
  - Add all events, conditions and exceeded/failed controls or barrier that occurred leading up to the event. Include people, H/W, S/W, policy, procedures

Build an Event Tree Structure



In Building an event tree

Capture each step/event

Identify initiating event / activity

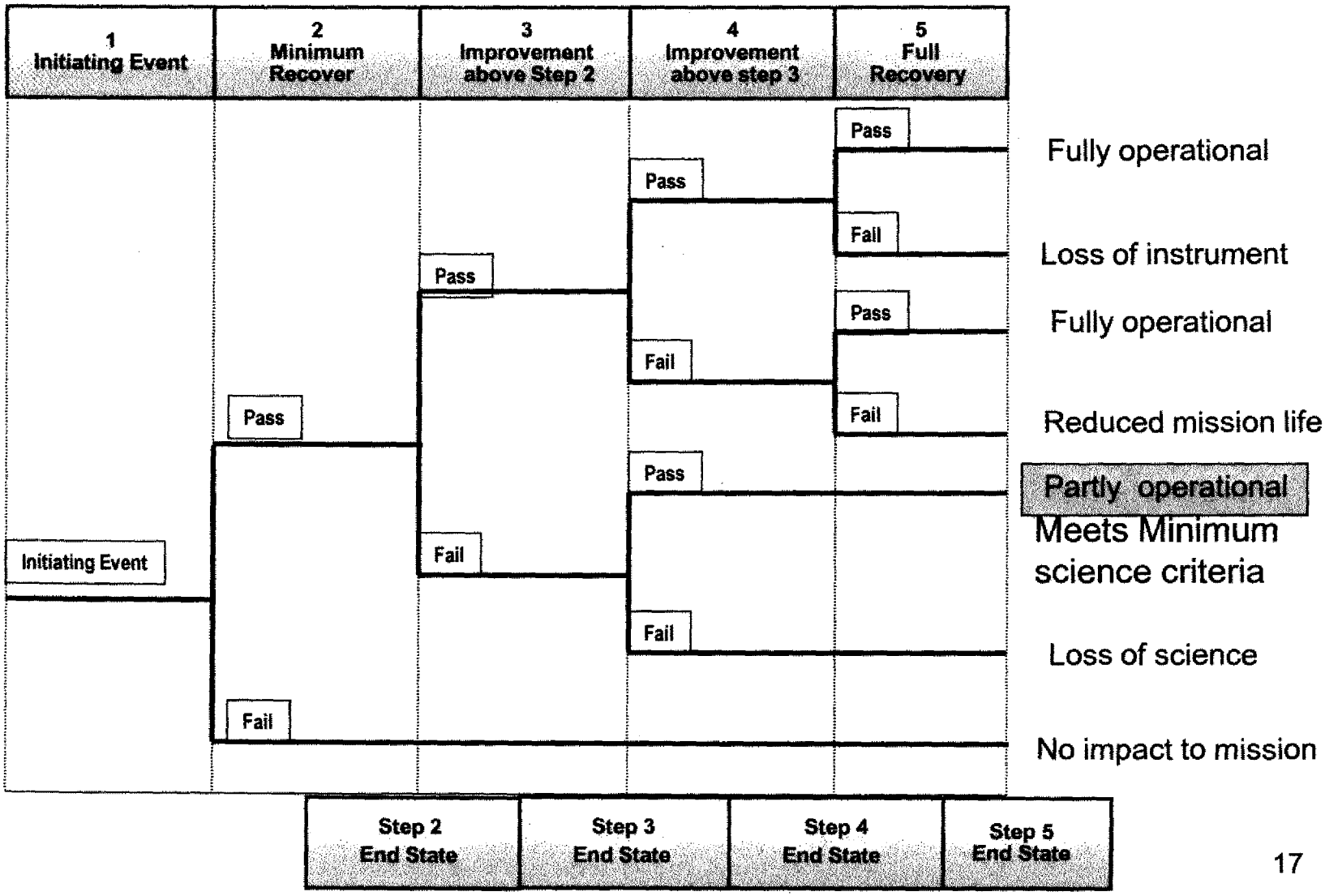
Identify the possible out comes of each step (End State)

Identify the risks to taking each step

If more than one end states was identified
decomposes branch until a single end state is found

Define recovery plan in terms of minimum to full success

Build an Event Tree Structure – Recovery Tool



Determining Recovery Options

- **Develop recovery options**
  - Insert recovery options in sequence flow diagram
    - Aids in determining if options will meet objectives
    - Aids in identifying other options
    - Aids in determining secondary effects to recovery actions

- **Prioritize recovery options**
  - Time critical
    - Mission, Performance, Science
  - Risk to Mission
    - What Can go wrong?
    - What options can be ground verified before execution?

- **Build an event sequence diagram** for planned recovery option(s)
  - Develop all steps for recovery with pass/fail criteria
  - Define Pass/fall criteria
    - Pass – document and move on
    - Fail – reenter failure analysis

Develop Recovery Options

- Brainstorm recovery options, consider
  - Fixing root or proximate cause
  - Developing work around

- Build sequence flow diagram for each option
  - Map options agents objectives
    - Look for secondary effects
    - Technique helps identify additional options

Prioritize Recovery Options

- Time critical
  - Mission, Performance, Science

- Risk to Mission
  - Determine the full and minimum recovery requirements
  - Decompose the recovery steps
    - What steps have to be successful
    - What can go wrong in each step
      - Identify the risk to the mission for implementing each step
    - What options can be ground verified before execution?

Fish Bone Axis

- *Possible Cause*
  - Proton hit corrupting or creating star centroid
- *Effect – failure*
  - Corrupted valid star used in star ID
- *Data Showed*
  - Corrupted quaternion due to star ID problems
- *What to do*

  Corrupted quaternion
  - Difference between current & previous quaternion is not so great.
  - If centroid & catalog stars are available; then, compute star measurement residuals & look for large residuals
  - Check for planets in the FOV or bright objects near the FOV

An Answer to the Example

- During high electron activity due to a geomagnetic storm
- S/C bus triggered Safehold and dropped into sun-reference pointing mode
- S/C main processor rebooted
- S/C lost Knowledge and Attitude
- All instruments were powered off
- Star tracker failed to reinitialize
- A soft-reboot was sent to star tracker
- S/C was commanded to inertial pointing mode

MOA for Mission Success

- An effective risk management process is critical to mission success
- A thorough test & verification program is also essential for mission success
- Test-as-you-fly, fly-as-you-test
- Institutional management sets policies, procedures for mission success
- Formal hand-off process (including all documentations) from pre-launch to mission ops team
- Consult appropriate experts and communication across institutional interfaces
- Telemetry coverage of critical events for analysis & feedback to other projects and missions
- Formalize and implement Independent Technical Review Team