Applications of Risk-based Decision Making in Aerospace Design

Michael V. Frank, Ph.D., P.E., CMC

riskexpert@ieee.org

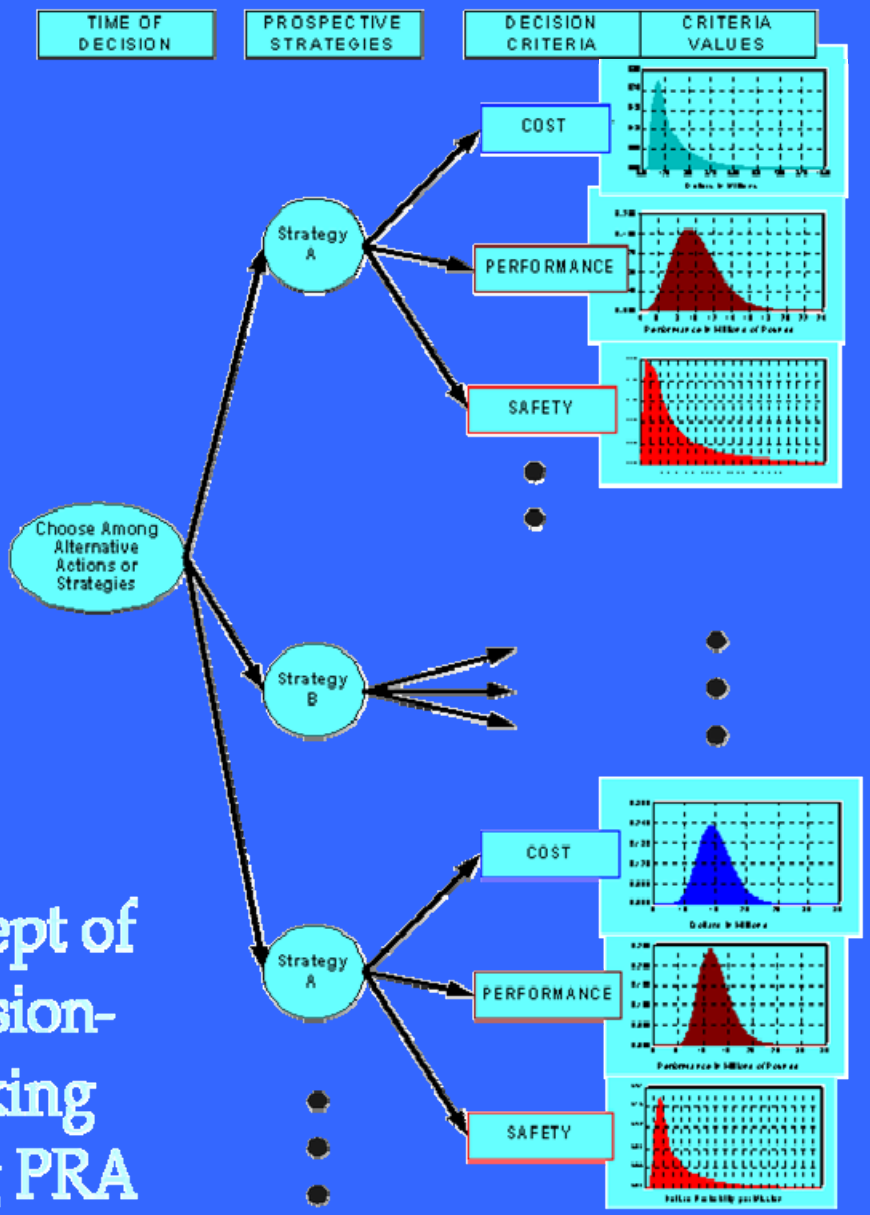
SFA Safe, Reliable, Affordable Technology

Definitions

- Risk (General): uncertainty in achieving an objective, goal, requirement, or other desired outcome.
- Safety[1]: a) Free from harm. b) Secure from threat of danger, harm, or loss.
- Safety Risk (as it relates to safety): Uncertainty in being free from harm, danger or loss (usually expressed as a probability of harm).
- Hazard: a precondition that has the potential to manifest or cause adverse effects.

[1] Webster's New World Dictionary

Risk-based Decision Framework

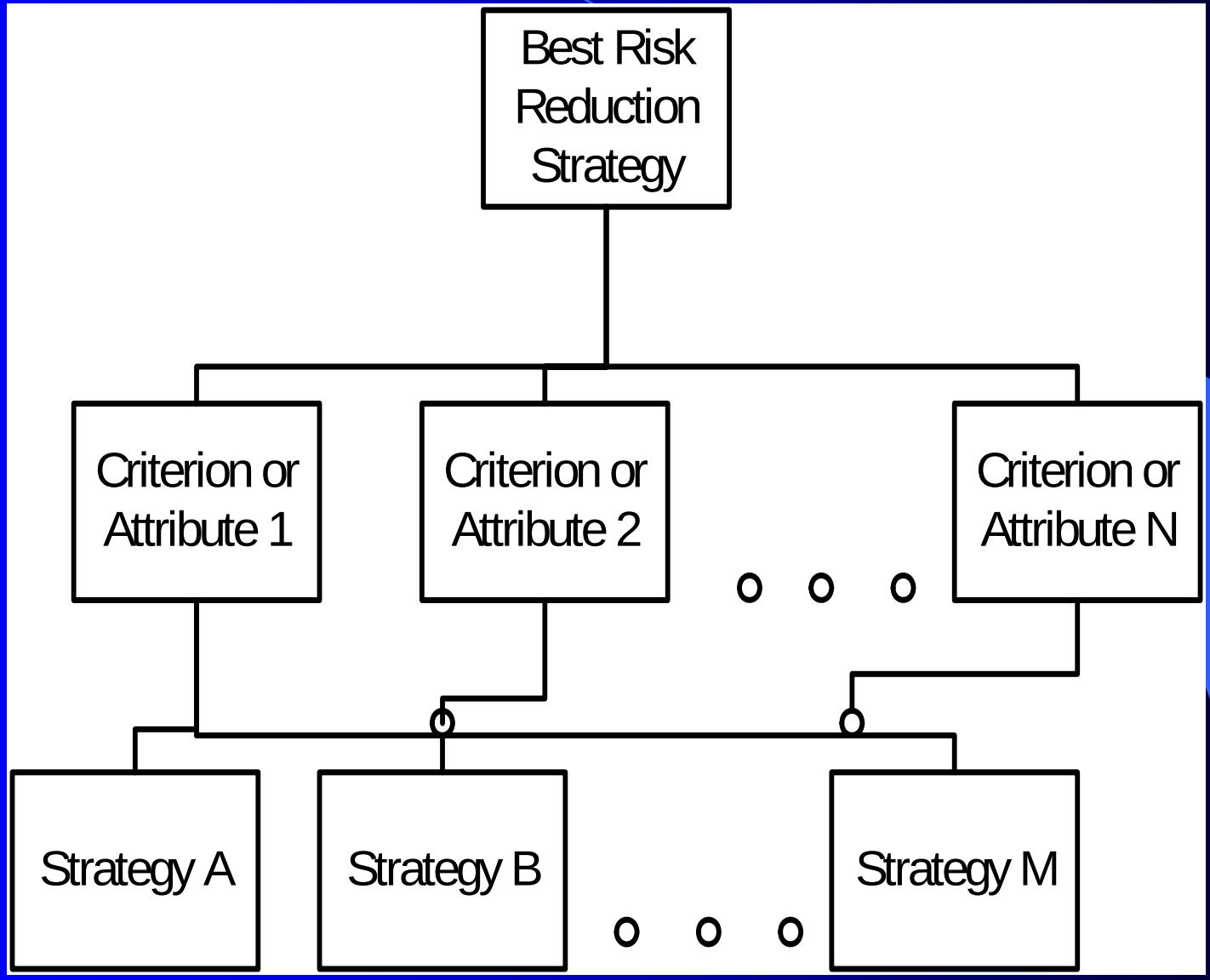


The decision-maker selects which set of criteria values are best.

Use Multi-criteria decision method such as Utility Theory or Analytic Hierarchy Process

Concept of Decision-Making Using PRA

Simple Analytic Hierarchy Diagram



Analytic Hierarchy Decision Process

- The risk analyses allow the ranking of each option with respect to cost and each option with respect to safety.
- The decision-maker decides on the relative importance of cost and safety.
- Then, the mathematics of the AHP (eigenvector of the maximum eigenvalue of the combined matrices) gives the overall rankings

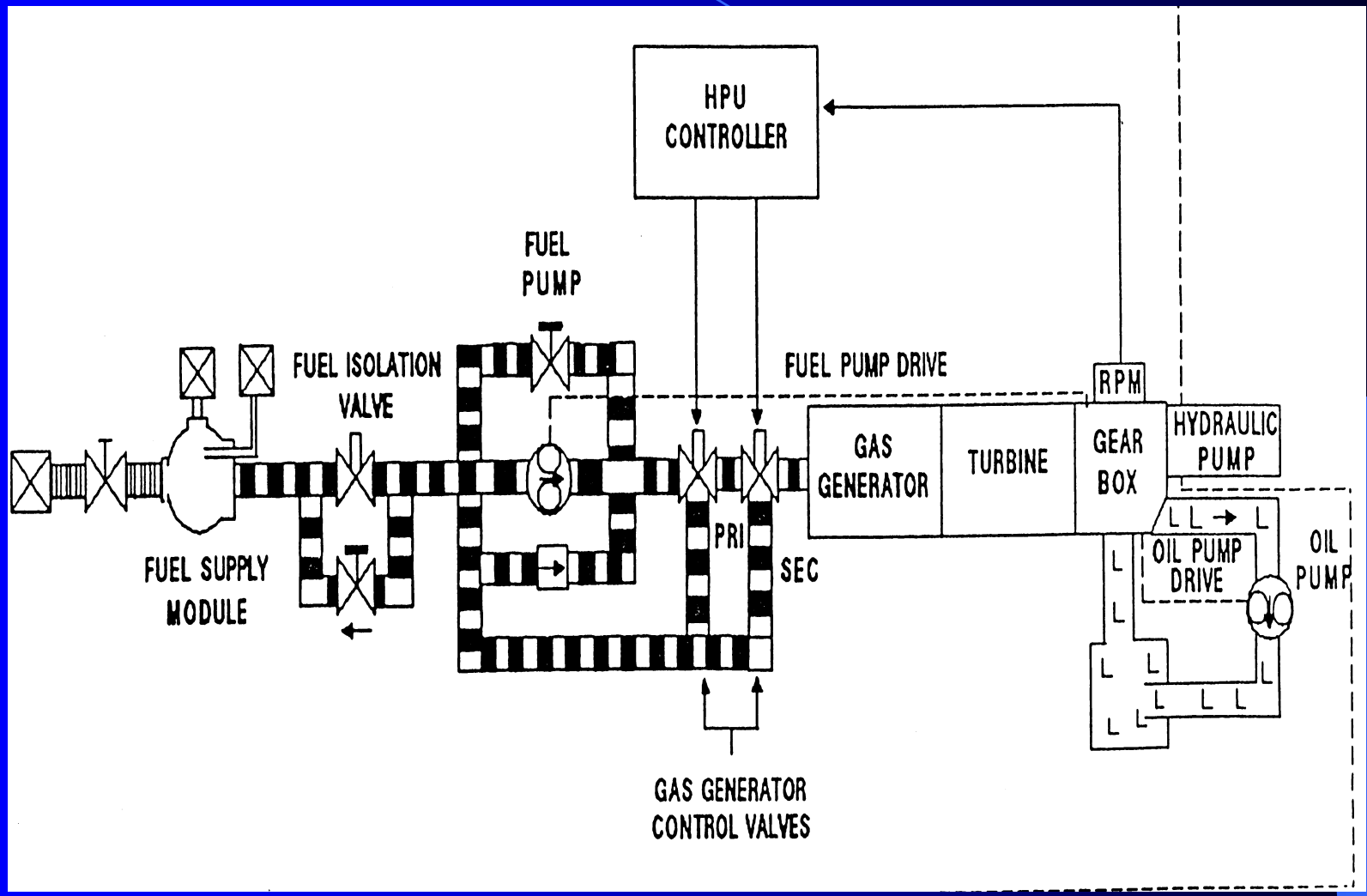
What Decisions?

- Find Best Risk Reduction Strategy (Shuttle APU)
- Go - No Go
- Improve Chance of Successful Mission (Mars Sojourner)
- Choose design concept (Micro-met spacecraft)
- Compare Against a Safety Goal
- Improve operation, inspection and maintenance (8'HTT)
- Improve Design Process
- Gain Confidence that System will Perform
- Prioritize Critical Items or Scenarios

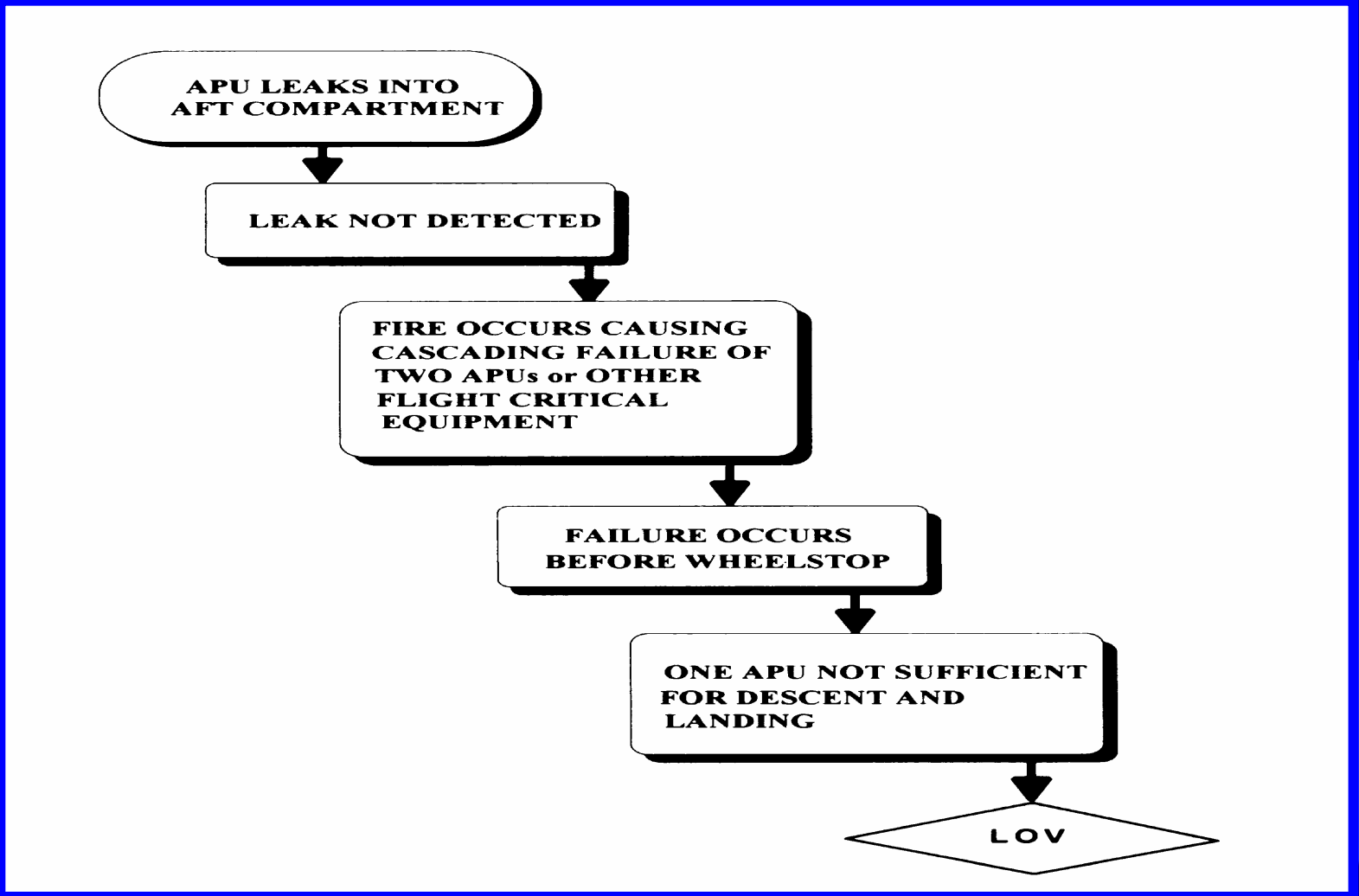
Best APU Risk Reduction Strategy

- Objective: Find the best alternative modification of the Space Shuttle APU considering both safety improvement and cost.
- Method: Using event sequence diagrams and Monte Carlo simulation develop a risk model for cost and safety for each alternative strategy. Use various decision analyses to decide on best overall alternative.

Typical APU Schematic



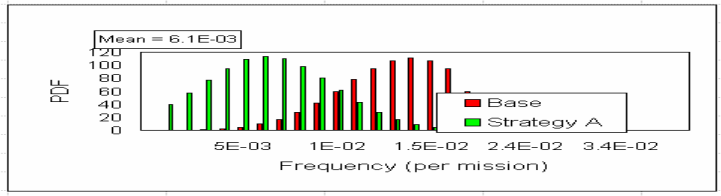
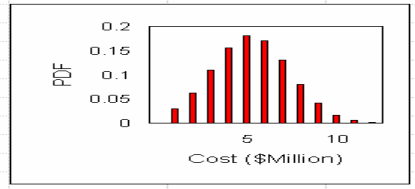
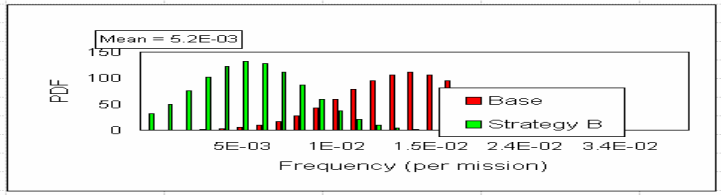
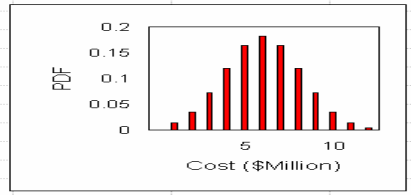
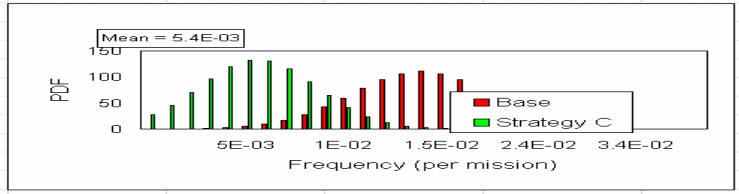
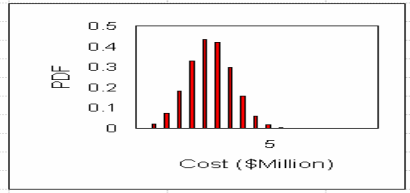
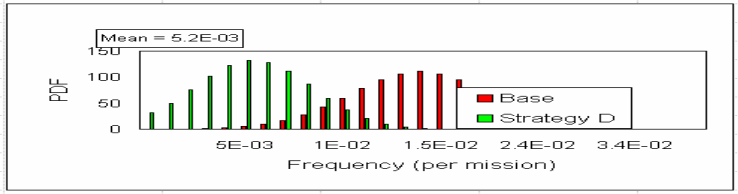
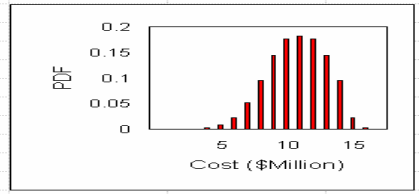
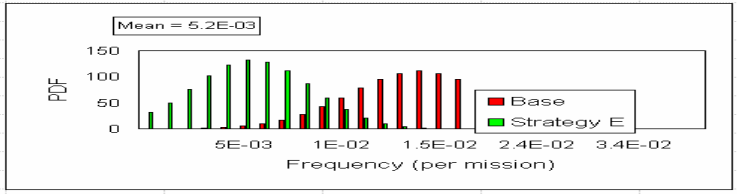
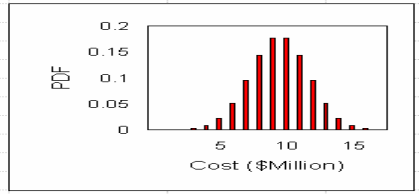
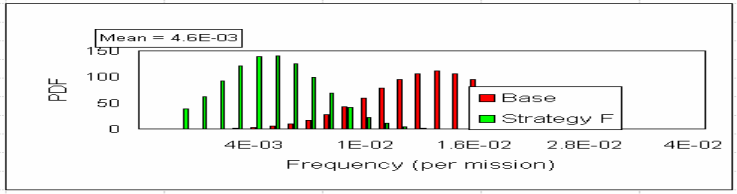
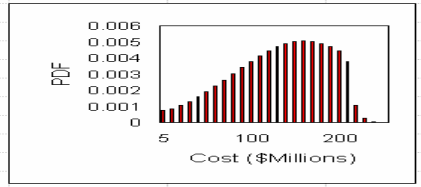
Highest Safety Risk Scenario



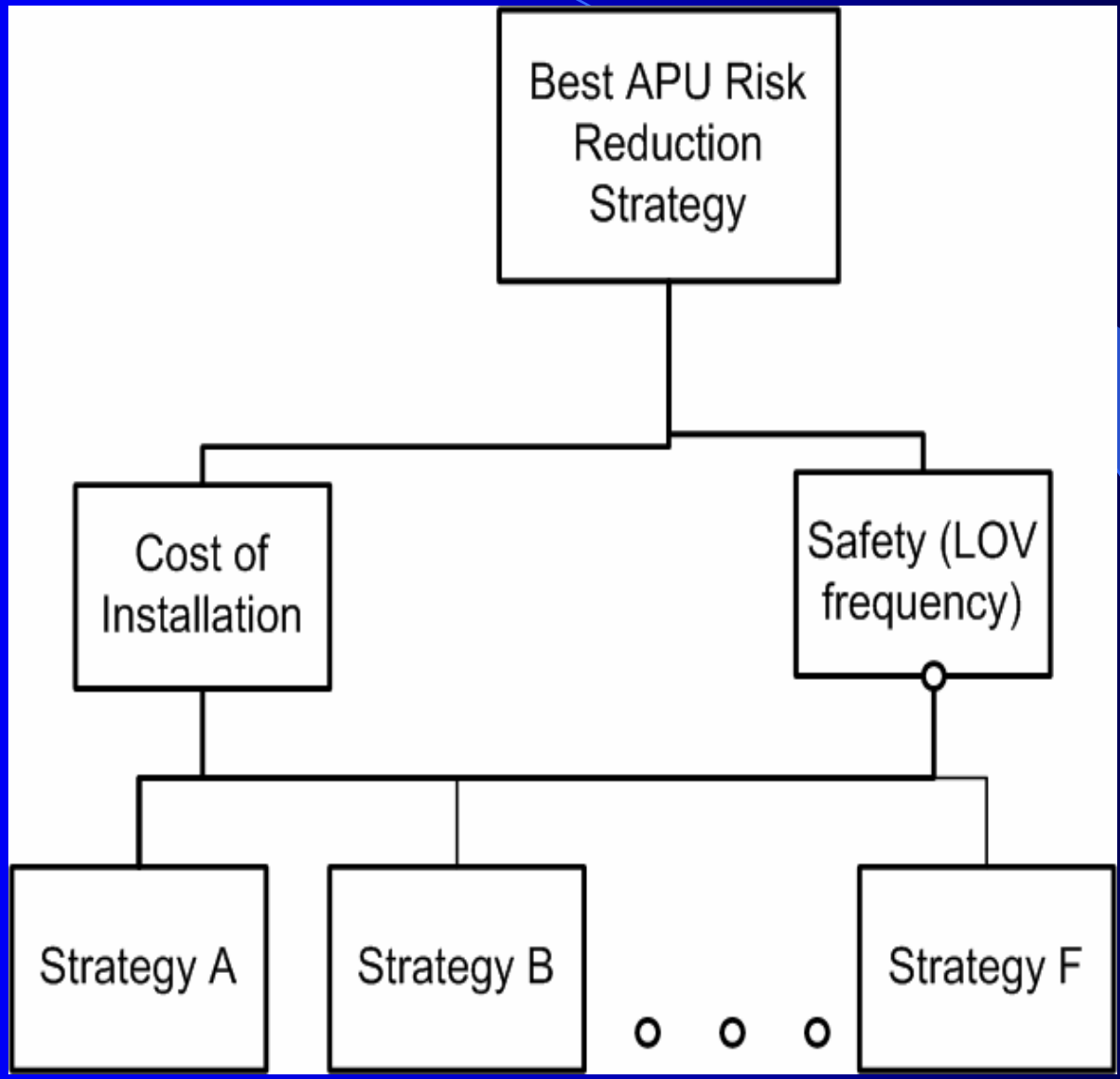
Find Best APU Risk Reduction Strategy

- Objective: Find the best alternative modification of the Space Shuttle APU considering both safety improvement and cost.
- Method: Using a baseline risk assessment of Space Shuttle APU, modify risk model for each alternative strategy. Obtain cost to implement each strategy. Use various decision analyses to decide on best overall alternative.

Results of Cost and Safety Studies

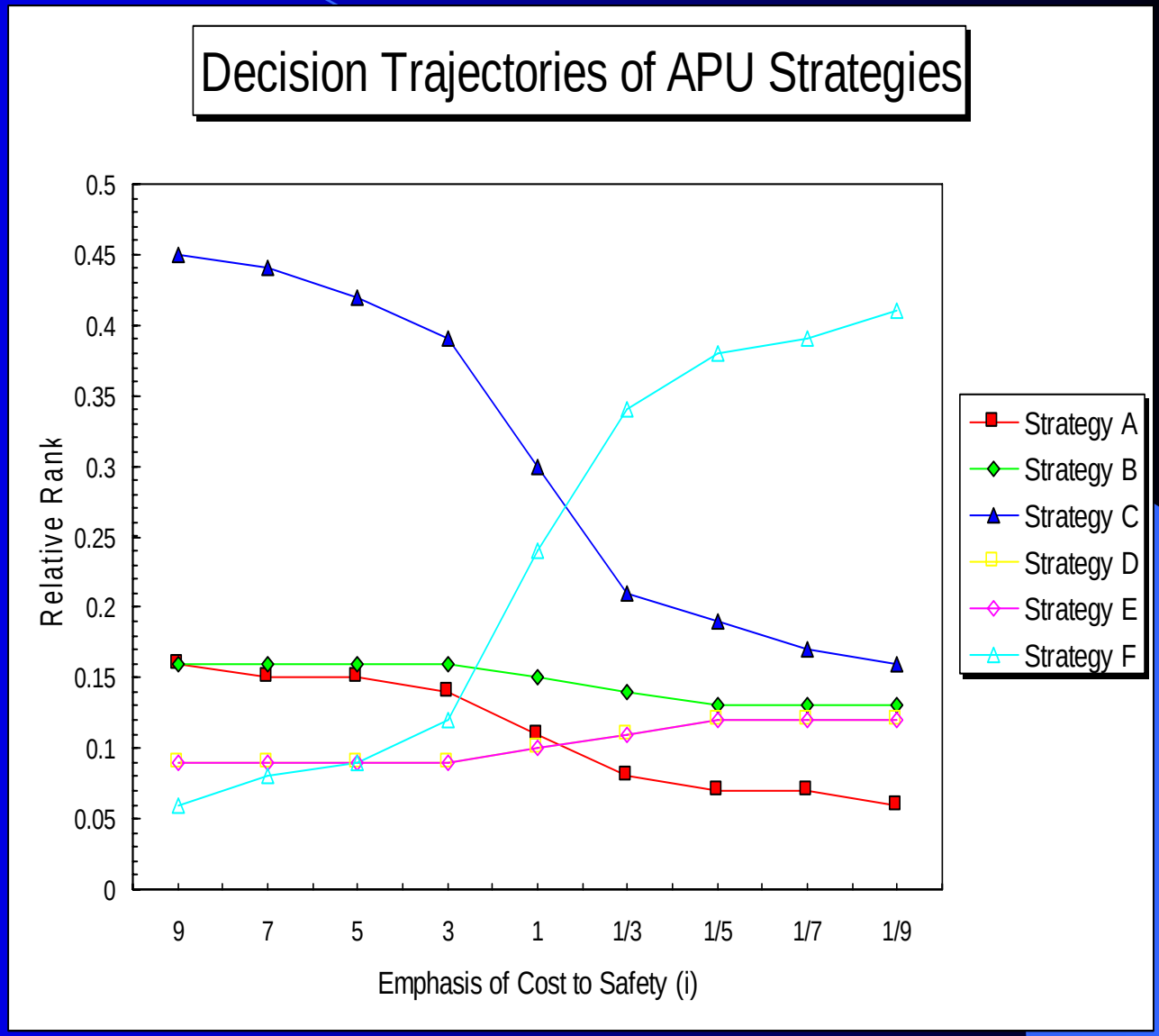
Strategy	Description	Safety of Strategy (Frequency of LOV)	Cost of Strategy
A	Leak Detection System		
B	Barriers		
C	Inert Aft Compartment		
D	Inert Atmosphere Inside Barriers		
E	Fire Supression Inside Barriers		
F	One of Three APUs Fully Capable of Descent and Landing		

Analytic Hierarchy Diagram



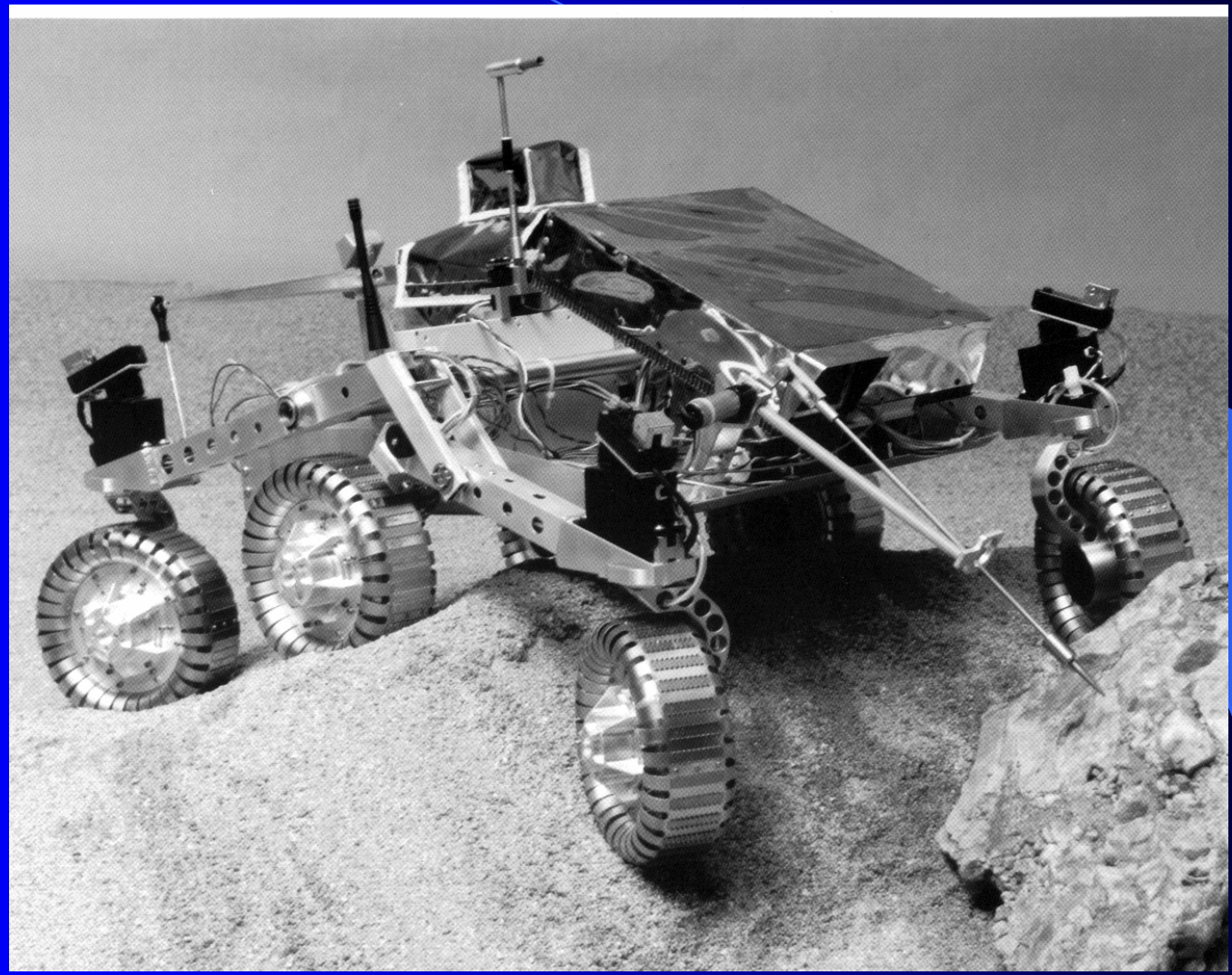
Findings

- There is no single best
- The results depend on:
  - Relative importance that the decision-maker assigns to cost v. safety



Mars Sojourner Integrated Mission Study

- Objective: Independent, alternative look at Sojourner's mission on Mars to find high risk areas that may have been overlooked by JPL.
- Method: Develop flow chart of Sojourner mission events. Develop fault tree of each major event to discover dominant modes and mechanisms.



Sojourner Features

- Length = 0.65 m
- Weight = 9 kg
- Top speed = 1 m/minute
- Acceleration = 0 to 1 m/minute in 0.2 seconds
- Six 2 watt electric motors, one on each wheel; Each wheel = 12.7 cm diameter
- Four wheel turning; 5 locked wheel rotation
- Energy usage = 100 watt-hour/day
- Solar power rechargeable Lithium-Thionol Chloride

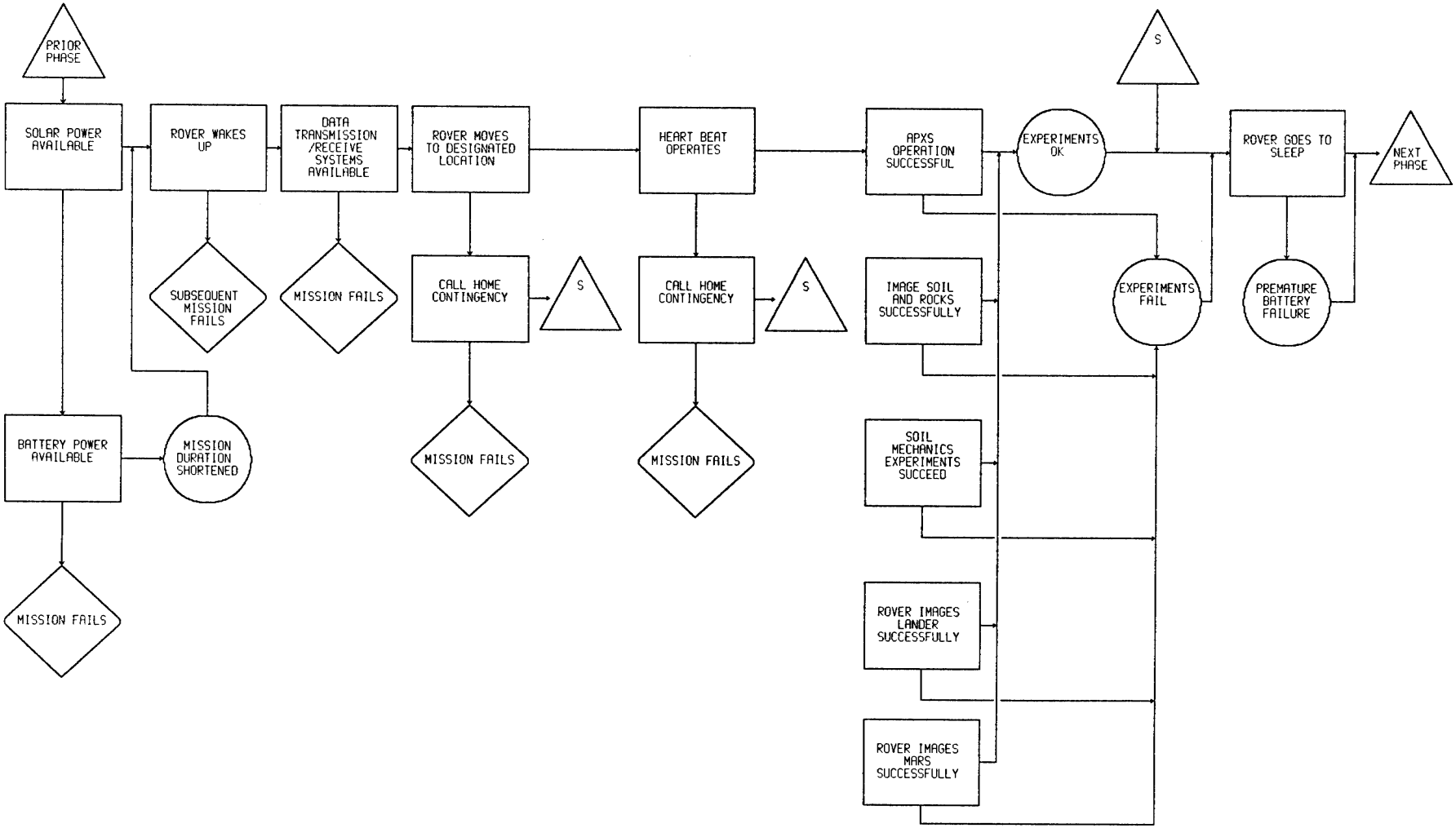
Sojourner Features

- Modem communication with Pathfinder Lander
- Sends “heartbeak” after each ½ length of travel. If can not “handshake” with Lander, then go to the spot of the last successful report.
- Directed from ground via Lander
- Limited ability to sense obstacles
- If can not get to the place where directed or can not avoid an obstacle after a few trus, stop and signal Lander.

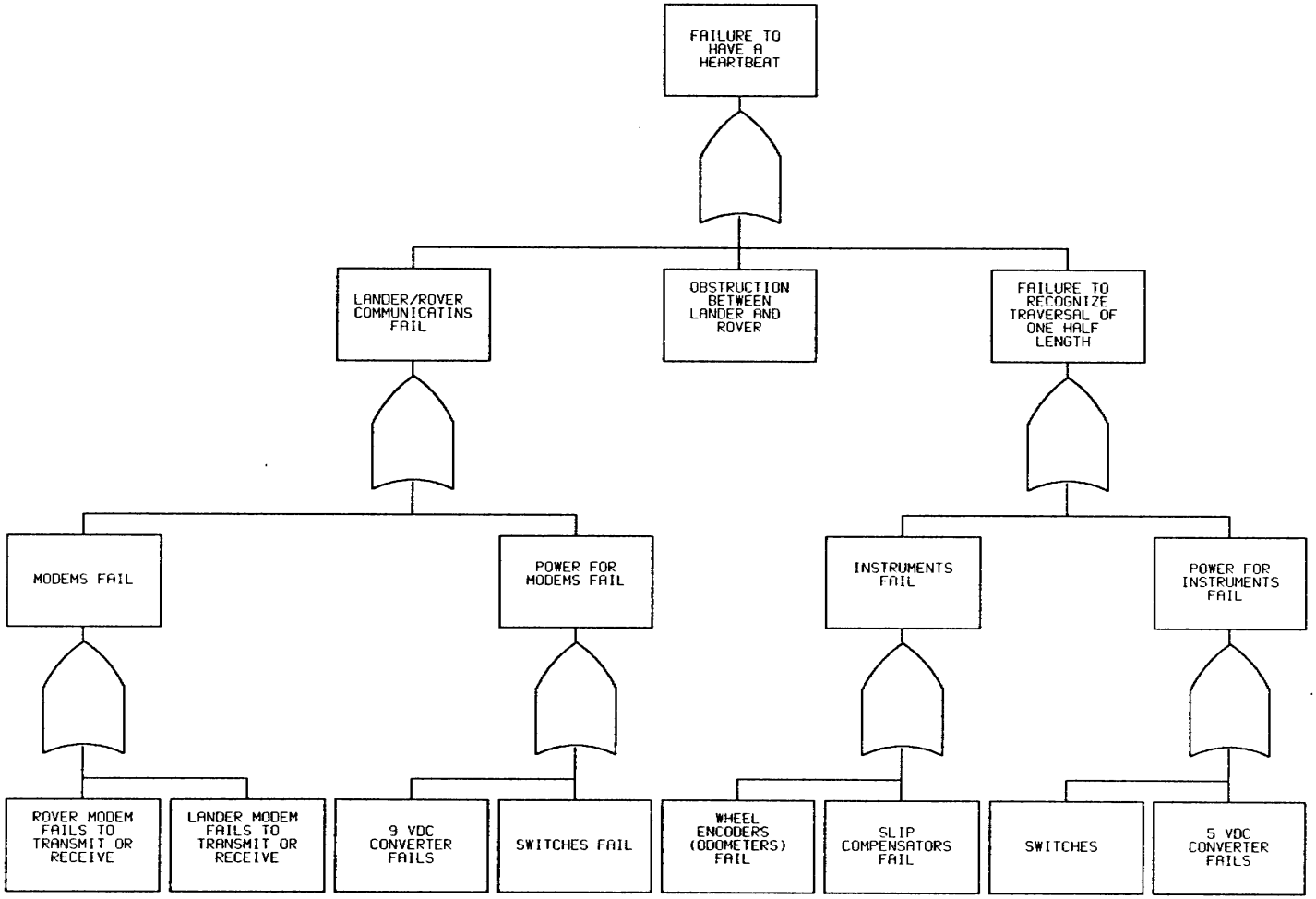
Other Features

- Climb hills up to 30 degrees
- Proximity sensor to avoid obstacles
- Take pictures
- Soil resistance tests
- Spectroscopy of soil or rock

Day Operations Event Sequence Diagram



Heartbeat Fault Tree



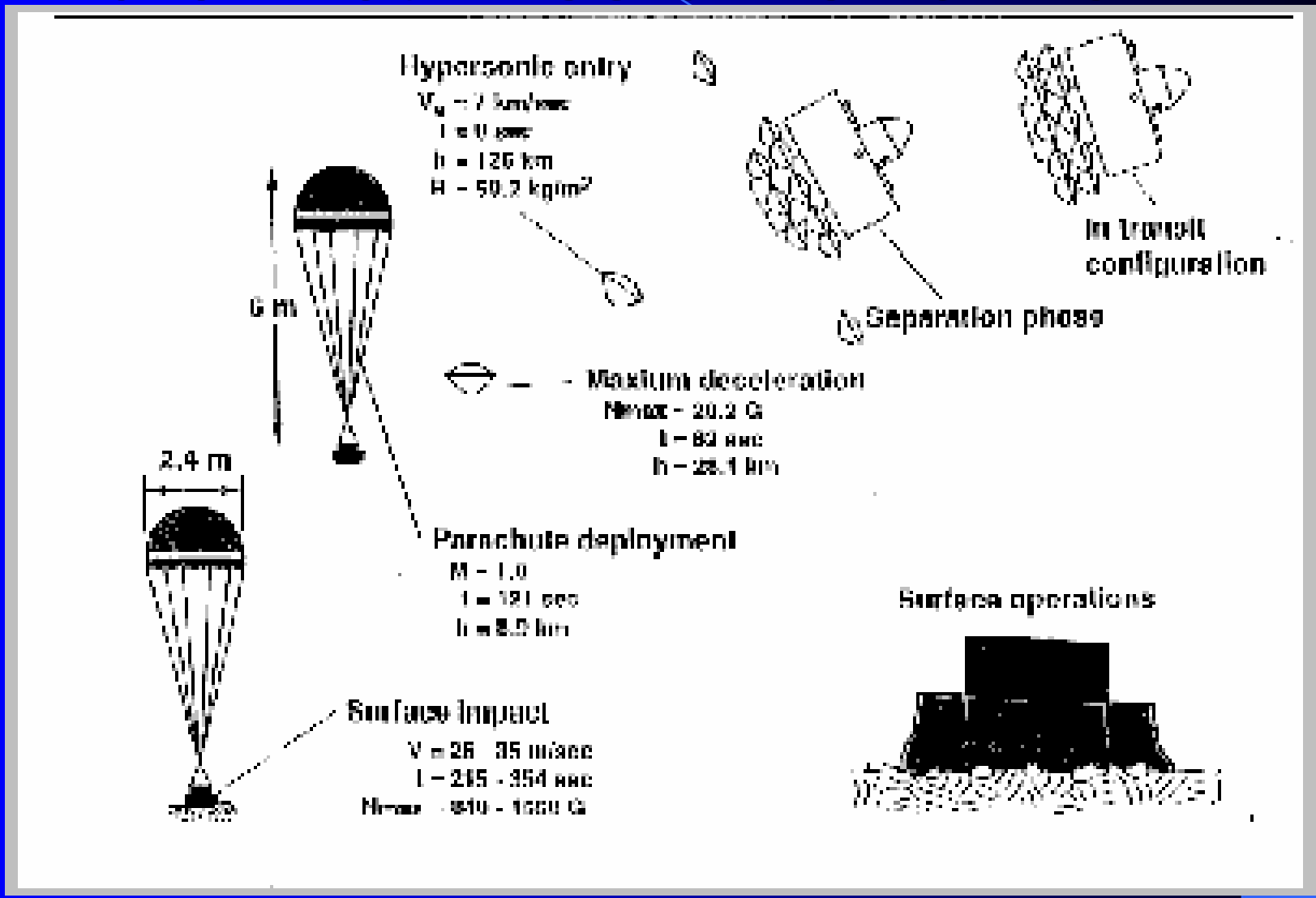
Sojourner Findings

- **Concept of "Graceful Degradation" Evident in Ability of Sojourner to Function With Failures**
- **Software can cause system freeze**
- Operations should be directed from ground as much as feasible....rather than relying on "intelligent software"
- Reallocate project Resources to improve Communications (even at the expense of software development)

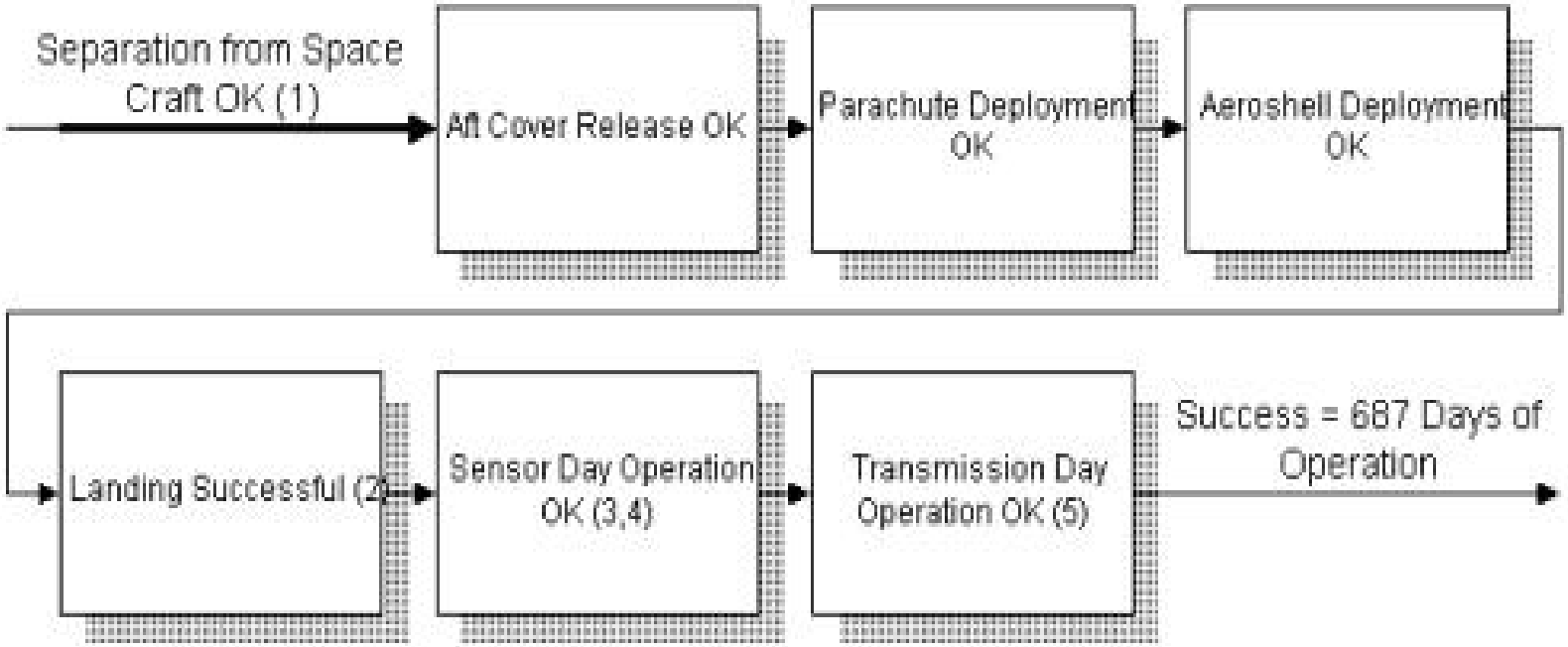
Micro-Met Mission to Mars

- Objective: Help develop mission architecture that will achieve goal of mapping Mars climate. Need 90% chance of successful operation of at least 12 meteorological stations operating on Mars for 2 Earth years.
- Method: Develop functional flow chart of mission. Develop and quantify fault tree for each function with uncertainties.

Micro-Met Mission Overview



Functional Block Diagram



(1) Assumes Controllers, CPU and Clock Initialized by Space Craft. No Latent Failures Owing to Launch, Cruise or Separation

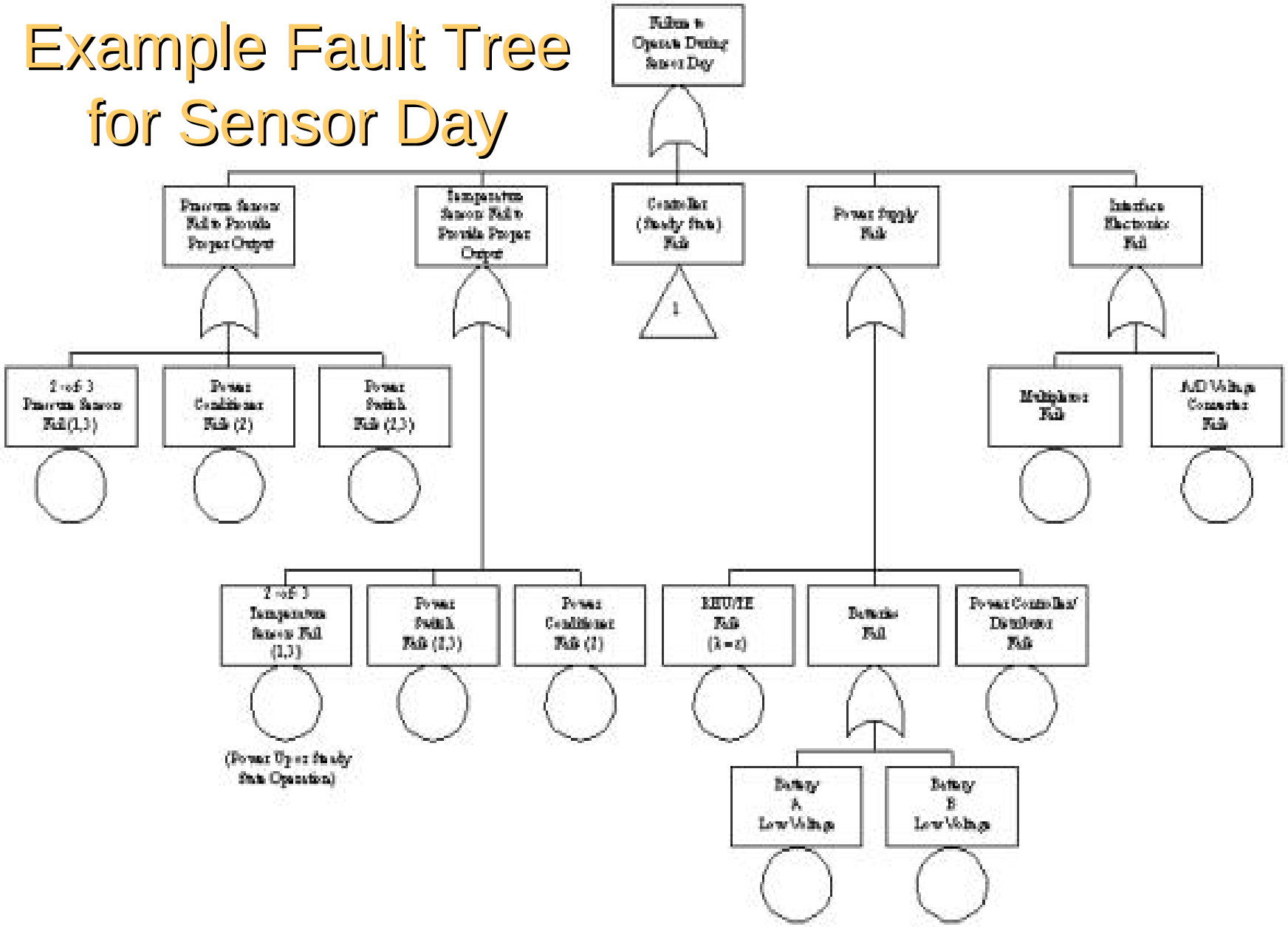
(2) Structural Failures of Lander Shells, Insulation and Aerobrakes Assumed to be Small Contributors to Unreliability

(3) LWRHUs and Thermoelectric Converter assumed to be Small Contributors to Unreliability

(4) This Includes all Active Components Except Those Used Only for Transmission. These Components Are Used Continuously for 687 Earth Days.

(5) This Includes Switches, Power Controllers, Receivers, and Transmitters Used Only for Transmission. These Components are Used Every 30 Days for a Total Intermittent Duty of 23 Days.

Example Fault Tree for Sensor Day



(1) Assumed for the base case that 2 of 3 sensors required

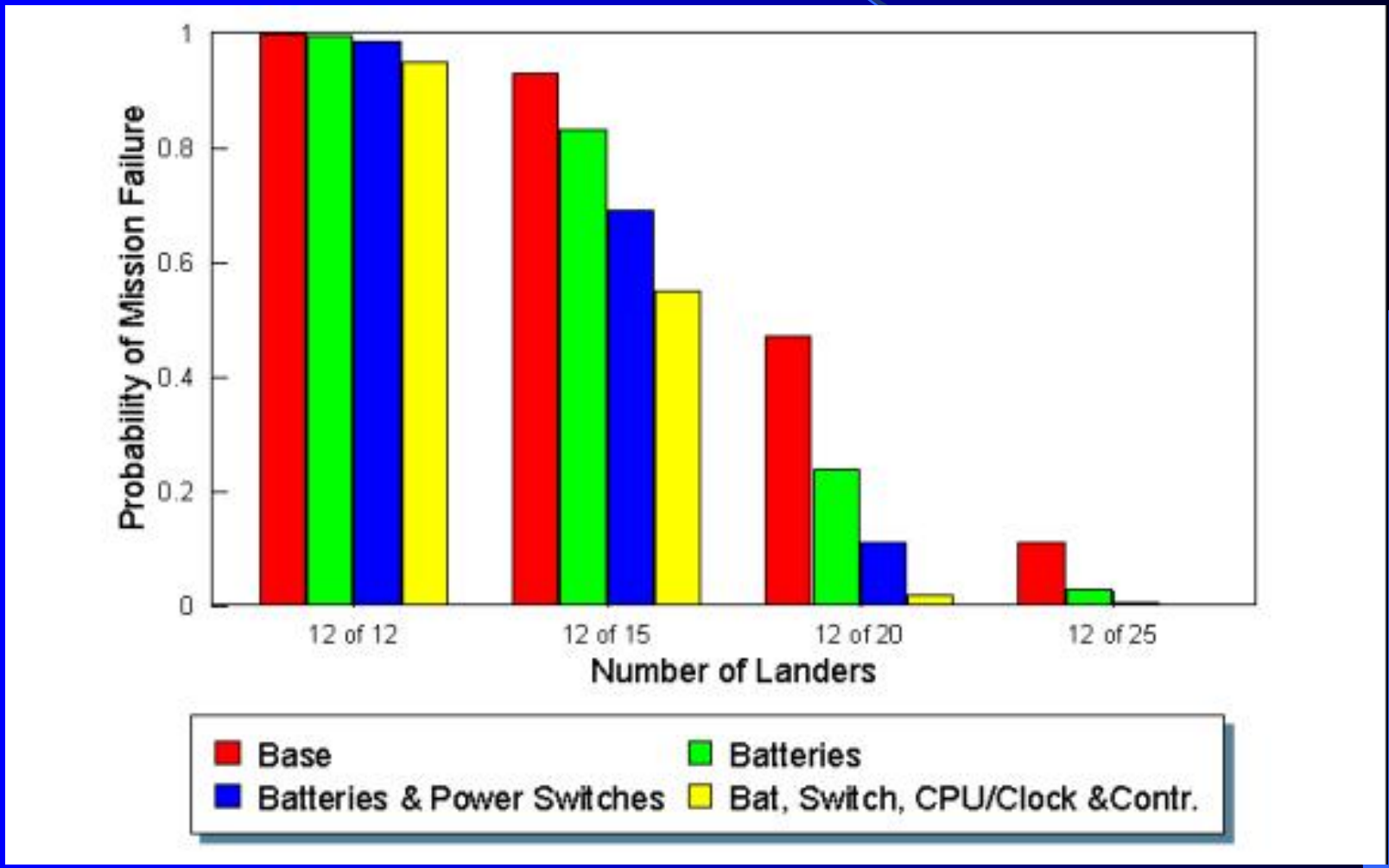
(2) Assumed separate power switch and power conditioner for each subsystem (per previous Mars mission design)

(3) 50 cycles/day (34320 cycles/mission); 1000 sec op. time/day (11430 min op. time/mission)

“Best of Breed” Strategy

- Wide variability in predicted reliability because of early phase of design
- Select only components with top 50% of reliability
- This can be done by screening manufacturer data and accelerated reliability testing

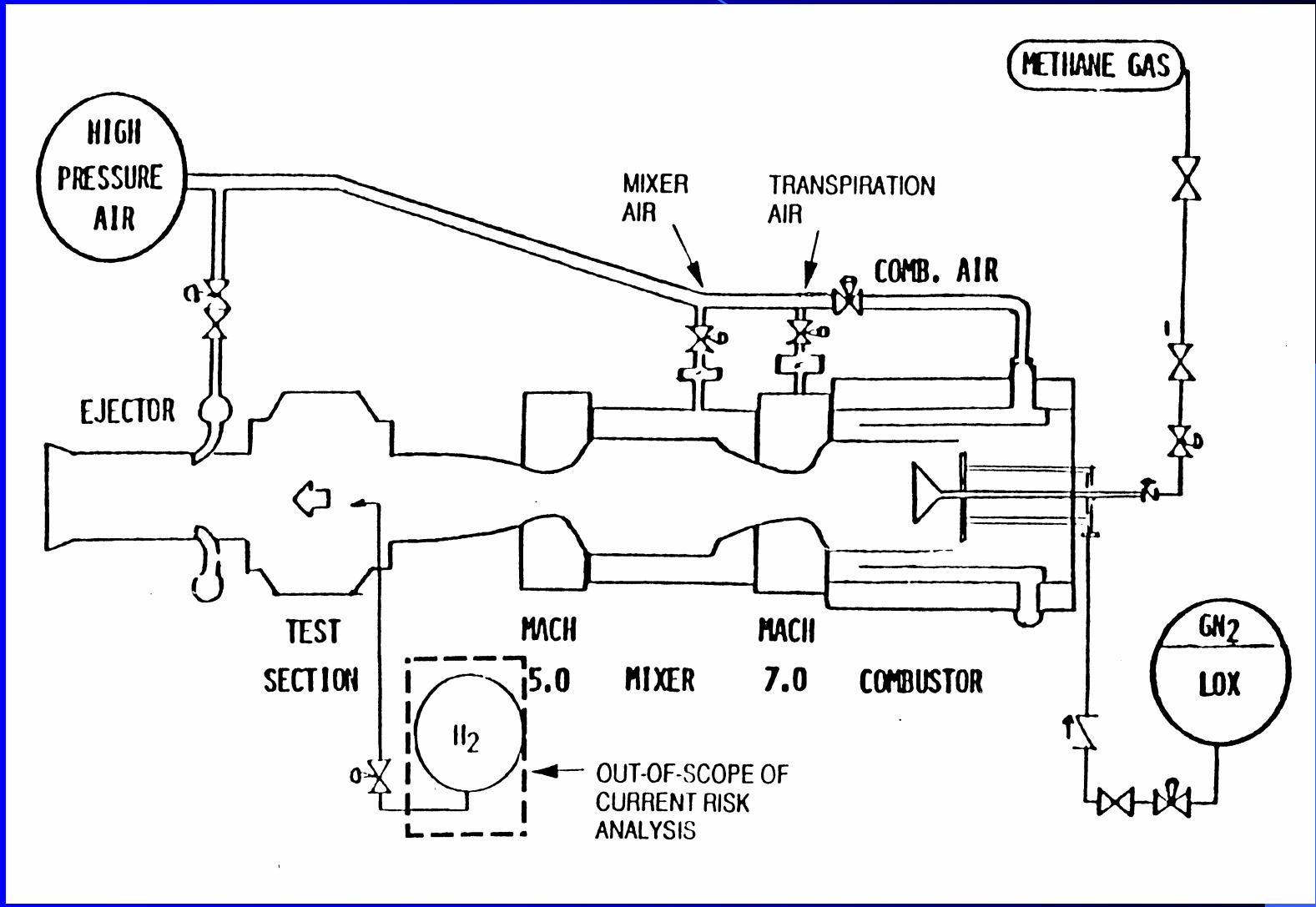
Suggested Number of Stations

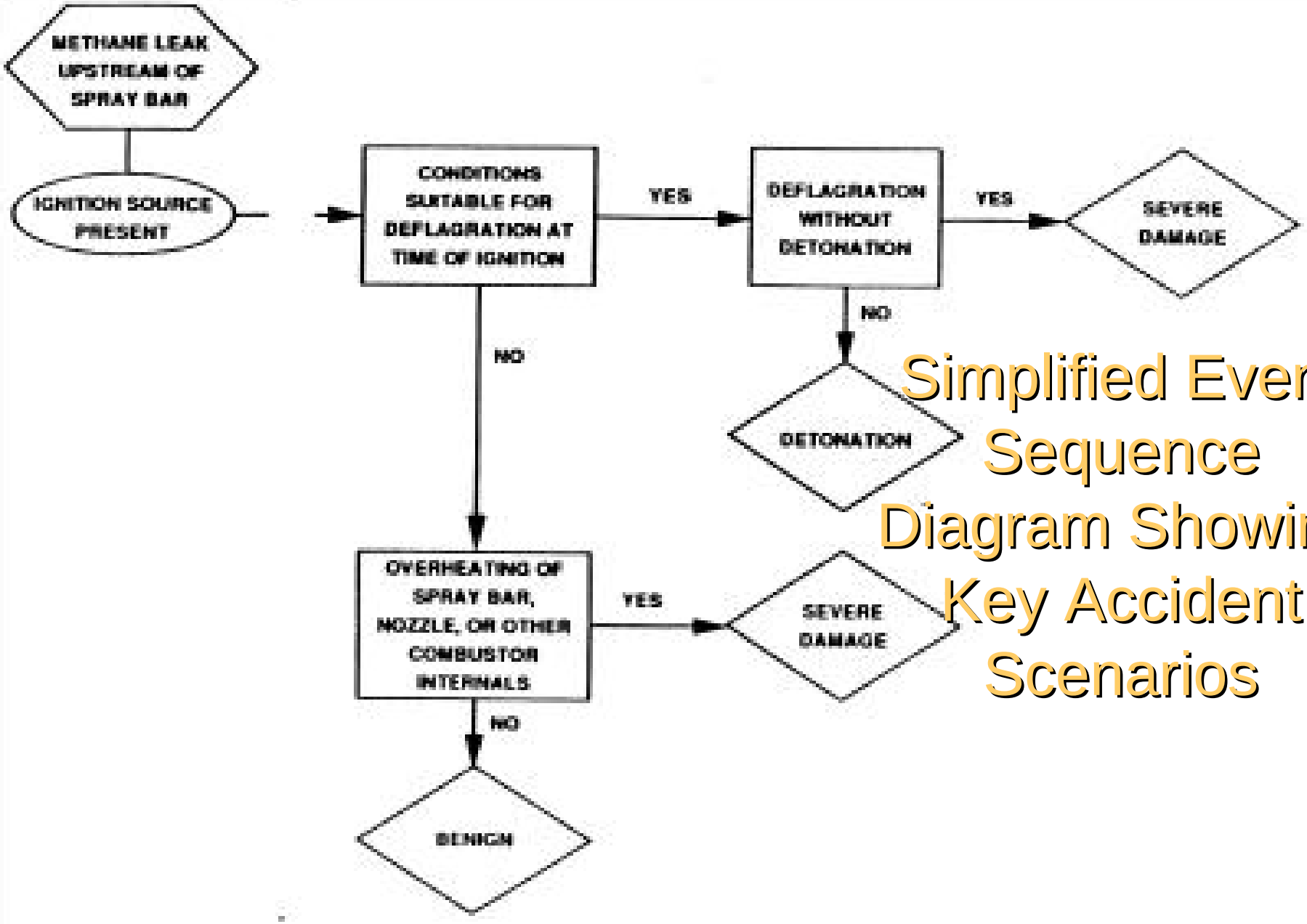


8'HTT Risk Assessment

- Objective: This is a high energy wind tunnel with a risk of deflagration, detonation, or overheating. Determine risk reduction strategies.
- Method: Comprehensive risk assessment using hazard analysis, master logic diagram, scenario diagrams, event trees, fault trees, and deterministic phenomenological studies on flames, deflagrations and detonations.

Simplified Representation of 8'HTT Wind Tunnel



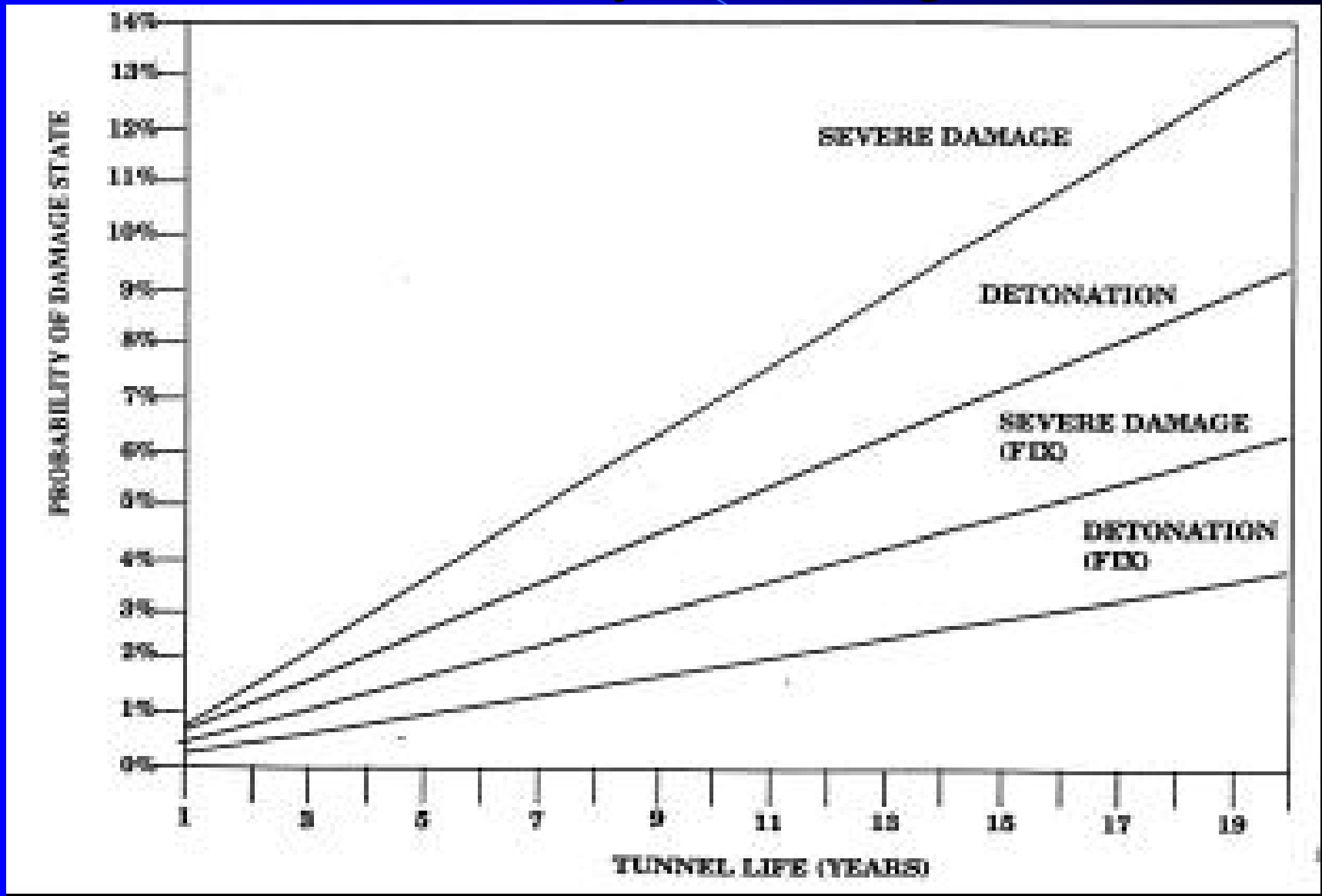


Simplified Event Sequence Diagram Showing Key Accident Scenarios

Most Feasible Risk Reduction Strategy

- Instrument for methane leakage
- Inspection program for fuel leaks
- Objective is to avoid a fuel rich mixture in tunnel, particularly at the beginning of a “run”.

Summary of Results
Probability of Damage



Acknowledgement

The event is supported by the Professional Services Development Assistant Scheme (PSDAS) of the Hong Kong SAR Government (Project Reference Number: 2005-2-12)

香港特別行政區政府工商及科技局
COMMERCE, INDUSTRY AND TECHNOLOGY BUREAU
THE GOVERNMENT OF THE HONG KONG
SPECIAL ADMINISTRATIVE REGION

Disclaimer

Any opinions, findings, conclusions or recommendations expressed in this material / any event organized under this Project do not reflect the views of the Government of the Hong Kong Special Administrative Region or the Vetting Committee for the Professional Services Development Assistance Scheme.

在此刊物上 / 任何的項目活動內表達的任何意見、研究成果、結論或建議，並不代表香港特別行政區政府及專業服務發展資助計劃評審委員會的觀點。