

Factors Contributing to Space System Failures and Successes

David Kaslow

Space System Failures and Successes

- Evolution of space systems development
 - Software design, hardware design and production techniques have been expanded and refined
 - Component and system modeling techniques are more comprehensive and accurate
 - Materials stronger and lighter
 - Standards have been defined and implemented
- Expectations
 - Knowledge of how to build a robust system should be increasing
 - Mission degradation and failures should gradually diminish
- Reality
 - Insurance rates / claims reflect not a decrease but rather an increase in malfunctions

Factors in Mission Malfunctions

Data Gathering Process

- Reviewed reported events for of hundreds of spacecraft
- Spacecraft Digest on-line database at www.stk.com
- Space News, Aviation Week & Space Technology, Press Releases, Govt Reports
- Mostly over the last five years
- Culled out and categorized over 120 examples of malfunctions

- Ground Test Damages Component
- On-Orbit Test Damages Component
- Flawed Ground Test
- Inadequate Ground Test
- Flawed Design
- Flawed Design Upgrade
- Improper Design Reuse
- Environment
- Launch - Hardware & Software
- On-Orbit - Hardware & Software
- Inattention to Events
- Single Event Upset

Factors in Mission Malfunctions

- Ground Testing Damages Component - HESSI Science Sat
 - Solar arrays were damaged during vibration testing
- On-Orbit Testing Damages Component - AMSC-1 Comm Sat
 - High power level on a test signal caused a power amplifier to burn out
- Flawed Ground Testing - Hubble Space Telescope
 - Flaw in test equipment compensated for incorrect curvature in primary mirror
- Inadequate Ground Testing - Mars Polar Lander
 - Not heard from after landing sequence was initiated
 - Likely cause was premature landing engine shutdown due to false signal that Lander legs had touched down

Factors in Mission Malfunctions

- Flawed Design - Cassini Spacecraft
 - Doppler shift between Cassini and Huygens probe not accommodated
 - Changes to telemetry system and flight path were made
 - Findings
 - Requirements not levied to cover Doppler shift
 - On board software that could have been changed to compensate for the Doppler shift was not modifiable
- Flawed Design Upgrade - Solar Arrays on BSS-702 Bus
 - Reflectors were added to increase solar power levels
 - After a while power levels gradually decreased – unknown cause
 - Design modified to remove reflectors, go to triple-junction solar cells, and add a panel

Factors in Mission Malfunctions

- Improper Design Reuse - Lewis Satellite
 - Slow spin after deployment - realized after out-of-contact for six-hrs
 - Insufficient solar power - batteries were depleted
 - Findings
 - Improper reuse of control system from TOMS-EP
 - Inadequate testing & insufficient operator monitoring
- Launch - Hardware & Software
 - Proton launch of Astra 1K
 - Left in incorrect orbit, likely due to contaminated fuel
 - Ariane 5 launch of Hot Bird 7 & Stentor
 - Failed to achieve orbit due to crack in a new version of a nozzle
 - Titan 4 launch of a DSP early warning satellite
 - Upper stages failed to separate because thermal tape wrapped around and electrical connector disabled its separation mechanism

Factors in Mission Malfunctions

- Inattention to Events - Mars Climate Orbiter
 - Was not heard from after orbital insertion burn
 - Arrived at Mars with a closest approach of 60 kilometers
 - Should have been no lower than 85 kilometers
 - Thruster table contained pound-foot-sec instead of Newton-sec
 - Findings
 - Analysis of thruster firing on the way to Mars would have uncovered incorrect units
 - Ground modeling of firing would have uncovered incorrect units
 - Navigation team did not have detailed attitude data and did not receive an independent expert review
 - Inadequate training on navigation characteristics and anomaly reporting

Factors in Mission Success

Usual Design Entities – Necessary But Not Sufficient

- Processes & procedures
- Concepts & requirements
- Architecture & design specs
- Design & production standards

Success-centric

Knowledge only from within

Many Problems Can Be Avoided

- Lessons-Learned Process
- Independent Review Process
- Risk Analysis
- Availability Analysis
- Failure Mode Analysis
- Recover Mechanisms

Address what can go wrong

Seek outside knowledge

*Knowledge Does Not Come From Specs
Knowledge Comes From Experience*

Factors in Mission Success

Lessons Learned Process

Analyze the problems that have occurred and recommend changes to methodologies

Usual Process

Lessons Not Learned

- Falls by the way-side during
 - Proposal negotiation
 - Development crunch
- Limited scope
 - Confined to expertise within the program
- Limited incorporation
 - Input to proposal and output from red-team reviews

Recommendation

- Cull from external sources
- Categorize according to program phase and type
- Develop mitigation and monitoring strategy

*Learn from Someone
Else's Problems*



Risk
Mgt

Factors in Mission Success

Review Process

Usual Short-Comings

- Customer review
 - At too high a level to uncover problems, lacks expertise
- Program level interval review teams
 - A few days review will not uncover low-level problems
- Worker level internal review teams
 - Limited time and less funding

Recommendation

- Built the review process into the Program Development Plan
- Use independent review team



Program
Dev Plan

*You Don't Know
What You Don't Know*

Factors in Mission Success

Risk Analysis

Likelihood of occurrence of an undesirable consequence

Types of Risk

- Cost, schedule and technical risks
- Program management risk
 - Shortcomings in funding, staffing, methodologies
 - Adverse effect on cost, schedule or technical capability

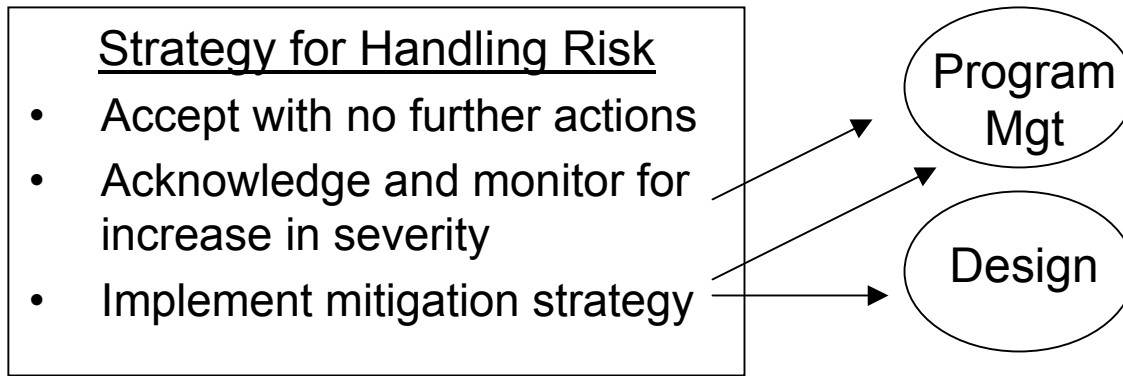
Process

- Apply across all program phases including proposal
- Apply across all program products
- Assess, rank and combine to establish severity of risk
 - Likelihood of occurrence
 - Consequence if risk is realized

INCOSE System
Engineering Handbook

Factors in Mission Success

Risk Analysis (cont.)



Mitigation Strategy Considerations

- Available funds, timeline and personnel to implement
- Intertwining of technical, cost and schedule risk
 - Technical risk mitigation
Mod design => Add effort => Cost risk or Schedule risk
 - Schedule risk mitigation
Relax requirements to simplify design => Technical risk

Risk Does Not Result in Failure - Inattention Does

Factors in Mission Success

Availability Analysis

Availability of 0.95 - System available for ops at least 95 % of the time

Allocate required availability

- Specify required availability, A, at system level
- Allocate from system, to sub-sys, to component, to H/W unit

Design each H/W unit

- MTBF - Mean time between failures
- MTTR - Mean time to repair
- Where $A = \frac{MTBF}{MTBF + MTTR}$

Calculate availability - bottom/up

- Assemble H/W units into components
 - Design in redundancy
 - Calculate component values of MTBF, MTTR & A
- Calculate sub-system and system values of MTBF, MTTR & A

MIL-STD-756B

Factors in Mission Success

Availability Analysis (cont.)

Compare calculated A to required A

- If it exceeds, consider design “relaxation” - if a cost savings
- If it falls short, modify design

Design

Considerations

- Specify different levels of availability
 - Non-mission critical
MTBF of 400 hrs & MTTR of 2 hrs => A of 0.995
 - Mission critical
MTBF of 1000 hrs & MTTR of 1 hrs => A of 0.999
- MTTR should consider total time
 - From getting repair personnel available
 - To restoring system operations

Ops & Maint

Time Spent Restoring is Time for Failure to Cascade

Factors in Mission Success

Failures Mode Analysis

FMECA - Failure Modes, Effects and Criticality Analysis

Evaluation of all probable failures

- Viewpoint of
 - Hardware item or
 - Functionality item or both
- From highest to lowest level
 - System to component
- Include effects of
 - Software failure & operator miscue

Define for each item

- Inputs & outputs
- Operating conditions & constraints
- What constitutes a failure on the output

Identify at each level

- Failure modes
 - The way the failure occurs and impact
- Single point failures
 - Results in failure of system
 - Not compensated by redundant or alternate functionality
- Extent of failure impact
 - Local level, next higher, highest
- Detection methods
 - In operations & maintenance modes
- Correction & mitigation
 - Design changes & operator actions
 - Material, procedures, ...

Factors in Mission Success

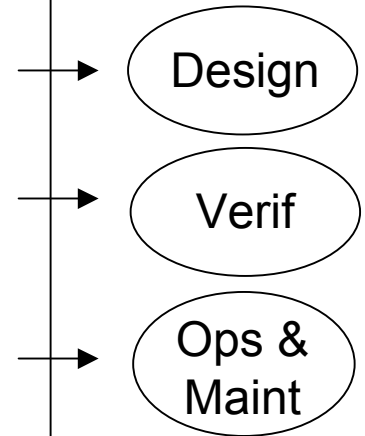
Failures Mode Analysis (cont.)

Construct criticality matrix

- A ranking of each failure mode for each item by:
- Level of severity
 - Catastrophic
 - Critical
 - Marginal
 - Minor
- Probability of occurrence
 - Frequent
 - Reasonably probable
 - Occasional
 - Extremely unlikely

Apply across program phase

- Evaluate, eliminate & mitigate failure modes
- Verify elimination & mitigation of failure modes
- Detect and mitigate failure modes



Majority of Design is for Normal Ops

Design to Avoid or Mitigate Failure Modes

MIL-STD-1629J

Factors in Mission Success

Failure Mode Recovery Mechanisms

Service satellites

Communication and navigation

- Relatively simple satellite processing/directing data
- Response is generally:
 - Failover to redundant component and resume operation
 - Automatic or directed by operator

Mission satellites

Imaging and science satellites

- Complex satellite executing command load sequences
- Response is generally:
 - Place the satellite into a protective mode
 - Await ground commanding for a reconfiguration and new command load

Factors in Mission Success

Failure Mode Recovery Mechanisms (cont.)

Ground systems failover scenarios

- Failover to standby hardware within operations environment
- Failover to alternate hardware within primary site
- Failover to alternate operational site

Mission satellite continuing ops through ground malfunction

- Command uplink
 - Execute on-board backup load if primary load expires
- Command generation
 - Uplink command load constructed ahead of time
- Schedule generation
 - Provide cmd gen alternate schedule constructed ahead of time

Factors in Mission Success

Mission Failure Recovery

Rebuild - Cluster

- The four satellites were destroyed in the inaugural Ariane 5 launch
- Rebuilt using spare, test and new components
- Two separate launches with launch insurance

Establish Secondary Mission

Wide-Field Infra Red Explorer

- Telescope cover released 3-days early – computer chip error
- Sunlight on cryostat evaporated coolant
- Secondary mission – study stellar oscillations using trackers

Execute Recovery Maneuvers

AsiaSat-3 (HGS-1)

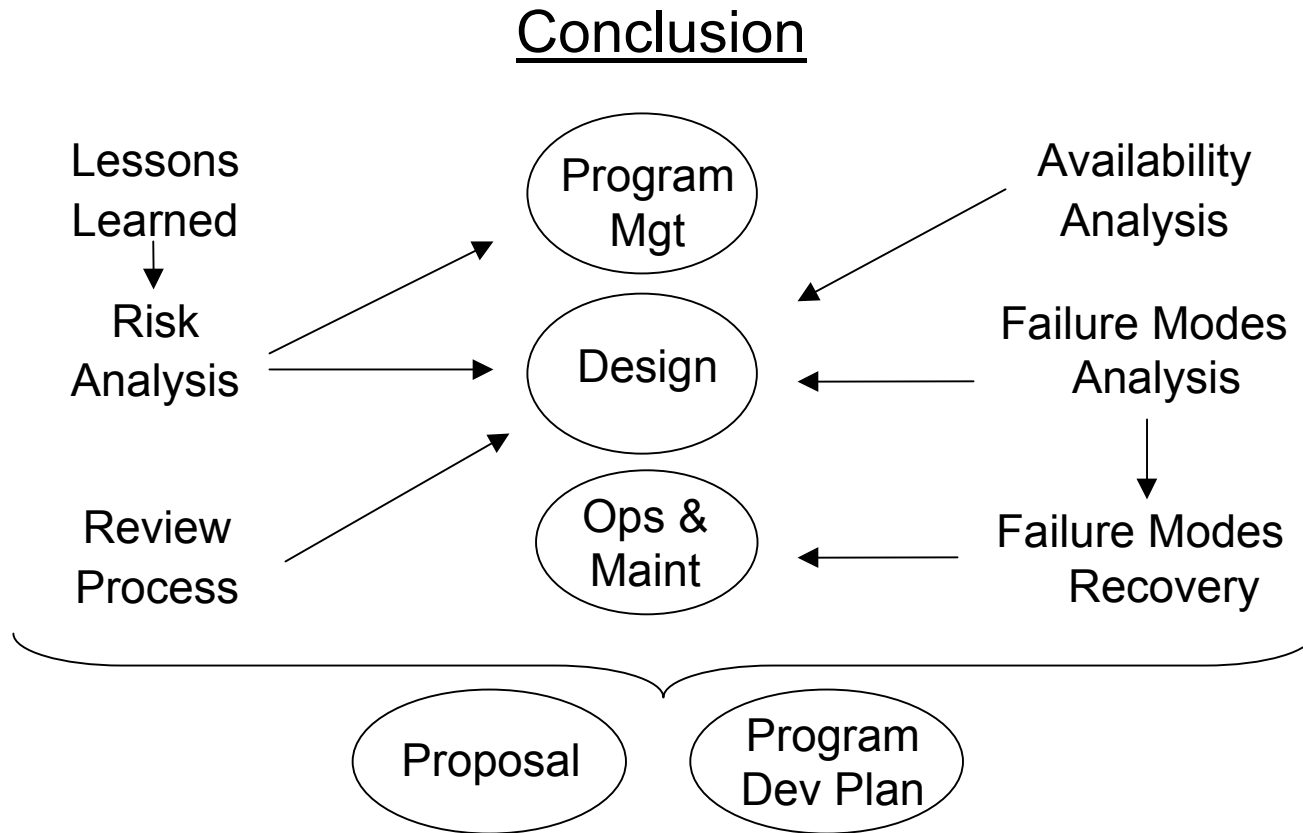
- Premature engine shutdown
- Use lunar flyby to return to geostationary orbit

Proposed

- On-orbit Geo-Comm Spare
- Space Tug

*Failure is Not Good
Failure to Recover is Worse*

Factors in Mission Success



- Design to accommodate degradation, failure and recovery
- Proposals and Program Development Plans must commit to direction, schedule and funding to building and operating a resilient system