Verification Module

Exploration Systems Engineering, version 1.0
Module Purpose: System Verification

♦ To define verification and validation for requirements and systems.

♦ To distinguish between verification and validation.

♦ To place verification planning and verification in context with the system development lifecycle and the Vee systems engineering model.

♦ To describe and provide examples of a verification matrix.

♦ To describe the four most common verification methods - test, demonstration, analysis and inspection.

♦ To describe typical environmental tests.

♦ To provide examples of the consequences of poor verification.
What Are Validation and Verification?

♦ **Validation** is a process of confirming that a set of requirements, design or system meets the *intent* of the developer or customer.

♦ **Verification** is a process of confirming that a requirement or system is *compliant*.
  ✓ In other words, system verification asks the question: Does the *system* meet its requirements?
  ✓ Requirements verification asks the question: Does the system indeed meet this particular requirement?
More on Requirements Validation

♦ Requirements Validation is the process of confirming the completeness and correctness of the requirements.

♦ Requirements Validation answers the question: “Are the system design requirements correctly defined and mean what we intended?”

♦ Requirements Validation tends to be oriented toward analysis.

♦ When does requirements validation take place?
  • Before design and during detailed design, i.e., mostly in Phase B and tapering down in Phase C
  • Ideally, completed prior to System Requirements Review (SRR)

♦ What is the importance of getting requirements validation right early in the project life cycle?
  • So when it comes time to verify the system, you are verifying to the right requirements.
  • Changing requirements late in the game - verification occurs in Phase D prior to launch - has negative impacts to cost and schedule.
More on System Validation and System Verification

♦ Validating a system: Building the *right system*: making sure that the system does what it is supposed to do in its intended environment. Validation determines the correctness and completeness of the end product, and ensures that the system will satisfy the actual needs of the stakeholders.

♦ Verifying a system: Building the *system right*: ensuring that the system complies with the system requirements and conforms to its design.
The Focus of This Module: Requirements Verification

♦ Requirements verification is done in Phase D - as an integral part of integration. In fact the right leg of the Vee is called ‘Integration and Verification’ (see following slide).

♦ But the preparations for verification begin with the development of the requirements.

♦ A preliminary plan for how a requirement will be verified is created when the requirement is generated. This is the preliminary verification matrix.

♦ After the design is complete, but before component verification begins a complete set of verification requirements are created and captured in the verification matrix.

♦ Verification requirements and plans are established with the completion of the critical design review (CDR).
Verification is Intertwined with the Integration of Components and Subsystems

- Mission Requirements & Priorities
- Develop System Requirements & System Architecture
- Allocate Performance Specs & Build Verification Plan
- Design Components
- Fabricate, Assemble, Code & Procure Parts
- Integrate System & Verify Performance Specs
- Component Integration & Verification
- Verify Component Performance

Decomposition & Definition Sequence
Integration & Verification Sequence

Time and Project Maturity
### Example Preliminary Verification Matrix for JWST

<table>
<thead>
<tr>
<th>Requirement ID</th>
<th>Requirement Description</th>
<th>Verification Technique</th>
<th>Verification Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MR-383</td>
<td>3.7.1.6.2 ISIM Reliability</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-110</td>
<td>3.7.1.7.1.1 Strehl Ratio</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-113</td>
<td>3.7.1.7.1.2.1 24 Hour Encircled Energy Stability</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-114</td>
<td>3.7.1.7.1.2.1.1 Conditions</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-115</td>
<td>3.7.1.7.1.2.2 Encircled Energy Long Term Stability</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-116</td>
<td>3.7.1.7.2 Strehl Ratio for Mid-Infrared Instrument</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-121</td>
<td>3.7.1.7.3 Stray Light at Near-Infrared Wavelengths</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-122</td>
<td>3.7.1.7.4 Stray Light From Thermal Emissions</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-371</td>
<td>3.7.1.7.5.1 Strehl Ratio For Moving Targets</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-123</td>
<td>3.7.1.8 Image Based Wavefront Sensing</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-124</td>
<td>3.7.1.9 Wavefront Error Correction Capability</td>
<td>D</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-391</td>
<td>3.7.1.10 Normal Operations</td>
<td>A</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-127</td>
<td>3.7.1.11.1 Observatory Event Logs</td>
<td>T</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-128</td>
<td>3.7.1.11.2 Command Authentication</td>
<td>T</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-129</td>
<td>3.7.1.11.3 On-Board Storage</td>
<td>T</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-130</td>
<td>3.7.1.11.3.1 Storage Capacity</td>
<td>D</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-133</td>
<td>3.7.1.11.3.2.1 Science Exposure Identification</td>
<td>A</td>
<td>T Observatory</td>
</tr>
<tr>
<td>MR-134</td>
<td>3.7.1.11.3.2.2 Science Observation Identification</td>
<td>A</td>
<td>T Observatory</td>
</tr>
<tr>
<td>MR-135</td>
<td>3.7.1.11.3.3 Simultaneous Onboard Storage</td>
<td>T</td>
<td>Observatory</td>
</tr>
<tr>
<td>MR-137</td>
<td>3.7.1.11.4 Common Data Bus, Point to Point, and Power Interfaces</td>
<td>I</td>
<td>Observatory</td>
</tr>
</tbody>
</table>

This verification matrix is useful since it identifies the requirement, the technique that will be used (inspection, analysis, demonstration or test) to verify it and the organization responsible for verification (e.g., observatory, ISIM or MSE).
The verification matrix specifies:

♦ Requirement
  ● Example: “Space vehicle first-mode natural frequency shall be greater than 35 Hz.”

♦ Associated verification requirement, including success criteria
  ● Example: “The space vehicle first-mode natural frequency shall be verified by test. The test shall conduct a modal survey of the vehicle using a vibration table. The test shall be considered successful if the measured first-mode is greater than 35 Hz.”

♦ Method of verification: Inspection, Analysis, Demonstration, Test
  ● Example: test

♦ Level verification is to be performed: Part, component, subassembly, assembly, Subsystem, System, Vehicle
  ● Example: vehicle

♦ Who performs the verification.

♦ The results of the verification as they become available.
## Example Verification Matrix

<table>
<thead>
<tr>
<th>Requirement No.</th>
<th>Document</th>
<th>Paragraph</th>
<th>Shall Statement</th>
<th>Verification Success Criteria</th>
<th>Verification Method</th>
<th>Facility or Lab</th>
<th>Phase</th>
<th>Acceptance Requirement</th>
<th>Preflight Acceptance</th>
<th>Performing Organization</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>xxx</td>
<td>3.2.1.1 Capability: Support Uplinked Data (LDR)</td>
<td>System X shall provide a max. ground-to-station uplink of...</td>
<td>1. System X locks to forward link at the min and max data rate tolerances 2. System X locks to the forward link at the min and max operating frequency tolerances</td>
<td>Test</td>
<td>xxx</td>
<td>5</td>
<td>xxx</td>
<td>xxx</td>
<td>TPS xxxx</td>
<td></td>
</tr>
<tr>
<td>P-i</td>
<td>xxx</td>
<td>Other paragraphs</td>
<td>Other “shall”s in PTRS</td>
<td>Other criteria</td>
<td>xxx</td>
<td>xxx</td>
<td>xxx</td>
<td>xxx</td>
<td>Memo xxx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S-i or other unique designator</td>
<td>xxxxxx (other specs, ICDs, etc.)</td>
<td>Other paragraphs</td>
<td>Other “shall”s in specs, ICDs, etc.</td>
<td>Other criteria</td>
<td>xxx</td>
<td>xxx</td>
<td>xxx</td>
<td>xxx</td>
<td>Report xxx</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Verification Plan

♦ System engineers develop a verification plan when writing the verification requirements.

♦ Importance:
  • To document a project’s approach to executing verification, including people, schedule, equipment, and facilities.
  • To ensure not breaking irreplaceable test units or endangering any of the staff.

♦ The verification plan includes system qualification verification as well as launch site verification, on-orbit verification, and post-mission/disposal verification.

♦ Support equipment is specified in the verification plan, including
  • Ground support equipment
  • Flight support equipment
  • Transportation, handling and other logistics support
  • Communications support infrastructure (e.g., TDRSS, DSN)
The Methods of Verification

There are 4 fundamental methods for verifying a requirement:

1. Inspection
2. Analysis
3. Demonstration
4. Test

Often joked that the top three verification methods are test, test, and test - to emphasize the importance of objective, measurable data in verifying a requirement.

Alternatively it is joked that one test is worth a thousand expert opinions - for equal emphasis.
Inspection

♦ Inspections determine conformance to requirements by the visual examination of drawings, data, or the item itself using standard quality control methods, without the use of special laboratory procedures or equipment.

♦ Inspections include a visual check or review of project documentation such as, drawings, vendor specifications, software version descriptions, computer program code, etc.

♦ Inspection includes examining a direct physical attribute such as dimensions, weight, physical characteristics, color or markings, etc.

♦ The kind of language used in the item requirement that usually indicates verification by inspection is:
  • “…shall be at least 24 inches long…”
  • “…shall have the NASA logo in accordance with…”
  • “…shall be painted white…”
Analysis

♦ Analysis is the evaluation of data by generally accepted analytical techniques to determine that the item will meet specified requirements.

♦ Analysis techniques: systems engineering analysis, statistics, and qualitative analysis, analog modeling, similarity, and computer and hardware simulation.

♦ Analysis is selected as the verification activity when test or demonstration techniques cannot adequately or cost-effectively address all the conditions under which the system must perform or the system cannot be shown to meet the requirement without analysis.

♦ The kind of language used in the item requirement that usually indicates verification by analysis is:
  • “…shall be designed to…”
  • “…shall be developed to…”
  • “…shall have a probability of…”
Demonstration

♦ Demonstration determines conformance to system/item requirements through the operation, adjustment, or reconfiguration of a test article.

♦ Demonstration generally verifies system characteristics such as human engineering features, services, access features, and transportability.

♦ Demonstration relies on observing and recording functional operation *not* requiring the use of elaborate instrumentation, special test equipment, or quantitative evaluation of data.

♦ The kind of language used in the item requirement that usually indicates verification by demonstration is:
  
  • “...shall be accessible...”
  • “...shall take less than one hour...”
  • “...shall provide the following displays in the X mode of operation...”
Test (1/2)

♦ Test is a verification method in which technical means, such as the use of special equipment, instrumentation, simulation techniques, or the application of established principles and procedures, are used for the evaluation of the system or system components to determine compliance with requirements.

♦ Test consists of operation of all or part of the system under a limited set of controlled conditions to determine that quantitative design or performance requirements have been met.

♦ Tests may rely on the use of elaborate instrumentation and special test equipment to measure the parameter(s) that characterize the requirement.

♦ These tests can be performed at any level of assembly within the system assembly hierarchy.

♦ The analysis of data derived from tests is an integral part of the test program and should not be confused with “analysis” as defined earlier.
Test (2/2)

♦ Testing is the preferred method of requirement verification and used when:
  1. Analytical techniques do not produce adequate results,
  2. *Failure modes* exist which could compromise personnel safety, adversely affect flight systems or payload operation, or result in a loss of mission objectives, or
  3. For any components directly associated with critical system interfaces.

♦ The kind of language used in the item requirement that usually indicates verification by test is:
  • “…shall provide 50 Hz…”
  • “…shall be settable over a range of 0 to 30 degrees C…”
  • “…shall not be larger than 10 microns, at once per rev frequency…”
Establishing Confidence With Environmental Test

- Verification is about establishing confidence that the system will perform in space.

- Because of the unique environment of space and the unique way of getting there, space systems go through rigorous ground-based tests that simulate the launch and space environments.

- To view general information and pictures for the Goddard Space Flight Center (GSFC) environmental test facilities and engineering: http://mscweb.gsfc.nasa.gov/549web/
# Key Space Environmental Tests

<table>
<thead>
<tr>
<th>Test</th>
<th>Purpose</th>
<th>Equipment/Facilities Required</th>
<th>Process</th>
</tr>
</thead>
</table>
| **Vibration & Shock Testing** | Ensure product will survive launch                                     | Vibration table and fixture enabling 3-axis testing, and/or Acoustic chamber                    | Do low-level vibration survey (a.k.a. modal survey) to determine vibration modes and establish baseline  
|                               | Comply with launch authority’s requirements                             |                                                                                                | Do high-level random vibration following profile provided by launch vehicle to prescribed levels  
|                               | Validate structural models                                             |                                                                                                | Repeat low-level survey to look for changes  
|                               |                                                                        |                                                                                                | Compare results to model                                                                                                                                                                             |
| **Thermal & Vacuum Testing**  | Induce and measure outgassing to ensure compliance with mission requirements | Thermal/vacuum chamber Equipment to detect outgassing (e.g. coldfinger or gas analyzer) as needed Instrumentation to measure temperatures at key points on product (e.g. batteries) | Operate and characterize performance at room temperature and pressure  
|                               | Ensure product will perform in a vacuum under extreme flight temperatures |                                                                                                | Operate in thermal and/or thermal vacuum chamber during hot and cold-soak conditions  
|                               | Validate thermal models                                               |                                                                                                | Oscillate between hot and cold conditions and monitor performance  
|                               |                                                                        |                                                                                                | Compare results to model                                                                                                                                                                             |
| **Electromagnetic Interference/ Compatibility (EMI/EMC)** | Ensure product does not generate EM energy that may interfere with other spacecraft components or with launch vehicle or range safety signals Verify that the product is not susceptible to the range and/or launch EM environment | Radiated test: Sensitive receiver, anechoic chamber, antenna with known gain Conduction susceptibility matched “box” | Detect emitted signals, especially at the harmonics of the clock frequencies  
|                               |                                                                        |                                                                                                | Check for normal operation while injecting signals or power losses |
**Typical Space Environmental Test Sequence**

1. Inspection (required before and after each event as appropriate)
2. Functional test (required before and after each event as appropriate)
3. Pressure/leakage (repeat after vibration/acoustic and modal survey)
4. Electro-magnetic compatibility (EMC) and susceptibility
5. Mass properties - center of gravity/moment of inertia
6. Fit check
7. Modal survey (repeat after each level of shock, random vibration and/or static load test)
8. Shock
9. Static load test
10. Acoustic and random vibration test
11. Separation test
12. Thermal cycling
13. Thermal Vacuum
JWST at JSC Chamber-A
Thermal - Vacuum Test Preparation

Vibration isolation system for suspension system. Six minor intrusions thru the Chamber.

Cryo-Position Metrology provided by photogrammetry with cameras mounted on windmills to provide conical Scanning.

Suspension system which holds the OTE support structure, CoCl and ACFs.

This vacuum chamber is 90’ high x 55’ diameter

Example of test equipment design and set-up.
Why we test => examples of “if only…”

Mars Polar Lander Failure

Most Probable Failure Cause -- Lander engines prematurely shutdown; lander crashed into Mars surface.

♦ Touchdown Sensing System was vulnerable to spurious signals generated at leg deployment, causing premature engine shutdown.

♦ Mars Polar Lander test program flaw
  • Touchdown Sensors wiring error in system test
  • System test not repeated with wiring correction

♦ Software design did not include detection/protection for spurious signals.

Lesson Learned: “Test as you fly, fly as you test.”
Example: NOAA-N’ on Turn Over Cart in Preparation for Test
**NOAA-N’ Spacecraft Falls at Lockheed 9/6/03**

As the spacecraft was being repositioned from vertical to horizontal on the "turn over cart", it slipped off the fixture, causing severe damage. The 18' long spacecraft was about 3' off the ground when it fell. The mishap was caused because 24 bolts were missing from a fixture in the “turn over cart”.

Two errors occurred.

First, technicians from another satellite program that uses the same type of “turn over cart” removed the 24 bolts from the NOAA cart on September 4 without proper documentation.

Second, the NOAA team working today failed to follow the procedure to verify the configuration of the NOAA “turn over cart” since they had used it a few days earlier.

**IMPACT ON PROGRAM/PROJECT AND SCHEDULE:** The shock and vibration of the fall undoubtedly caused tremendous damage. Significant rework and retest will be required. NOAA-N’ was planned for launch in 2008.

**CORRECTIVE ACTION:** Lockheed Martin formed an Accident Review Team with GSFC participating. The immediate actions concerned safety (preventing the spacecraft from rolling, discharging the batteries, and depressurizing the propulsion system). NOAA-N’ was under guard, all records were impounded, and the personnel interviewed. After the safety issues were addressed, attention was focused on assessing the damage to the spacecraft.
Oops - The NOAA-N’ Spacecraft is Dropped
The NOAA-N’ Spacecraft is Dropped
The NOAA-N’ Spacecraft is Dropped
NOAA N-PRIME Mishap Investigation

Final Report

September 13, 2004
NOAA-N’ Conclusion: The $135 Million Mistake

♦ It will cost an estimated $135 M to rebuild the spacecraft's main section and two damaged instruments. No one was injured in the incident.

♦ The board faulted an unidentified engineer who did not look at the cart's configuration but instead relied on paperwork from a prior operation. "Had he followed procedures, the unbolted adapter plate would have been discovered and the mishap averted," the report said. "Errors were also made by other team members, who were narrowly focused on their individual tasks and did not notice or consider the state of the hardware or the operation outside those tasks.

♦ On October 4, 2004, NOAA announced it reached an agreement with Lockheed to finish the satellite.

♦ Lockheed will contribute all profits it earned from the contract to rebuild the spacecraft and complete the work on a cost-only basis.

♦ Originally, NOAA N’ was to be placed in storage awaiting a March 2008 launch. NOAA N’ was successfully launched on 6 February 2009.
Module Summary: Verification

♦ Validation - Did we build the right system?
♦ Verification - Did we built the system right?
♦ Requirements validation - Are the requirements complete, consistent, SMART and do they capture the intent of the system?
♦ Requirements verification is about establishing confidence that the system will perform in its intended environment.
♦ Requirements are verified by test, demonstration, analysis and inspection.
♦ Space systems go through rigorous ground-based tests that simulate the launch and space environment.
♦ Using heritage designs can save development time and money, but they should be validated and verified as if they represented new hardware.
♦ Simple procedural errors - like borrowing another project’s bolts - can lead to multi-million dollar (or life threatening) accidents.
Backup Slides for Verification Module

Additional Note:
- The first 5 slides in backup pertain to the Genesis re-entry mishap.
- These slides are also included in the Design Fundamentals module regarding design heritage.
- They emphasize the summary point — Using heritage designs can save development time and money, but they should be validated and verified as if they represented new hardware.
Stardust – Utah Landing
When the Genesis spacecraft returned to Earth on September 8, 2004, the parachutes failed to deploy.

The spacecraft plunged into the Utah desert at 200 mph and broke apart.

The redundant sets of switches controlling parachute deployment failed to respond to reentry deceleration because both sets were installed backwards as specified in the design.
G-Switch Orientation

Acceleration Vector Required for G-Switch to Function

Actual Aerodynamic Braking Force Direction

Mounting Base of AU

Switches were Reversed!
The Genesis String of Events

♦ Schematic copied from Stardust
♦ Box CDR lacked technical content
♦ Verification requirements not clear
  • Centrifuge test expected (in CDR package), but not required. Verification matrix had test, but no detail
  • Systems Engineering did not have to sign off on Subsystem plans
♦ Designer verified **function** (open/close) of switches; Systems Engineering believed **orientation** of switches were verified
♦ Electrical designer incorrectly performed orientation verification via Mechanical drawing inspection
♦ Red Team review assumed design was correct because it was a “heritage” design
♦ Systems Engineering did not close the loop with the designer
  • Systems Engineering not required to review test result

Breakdown
♦ Heritage
♦ Design Review Weakness
♦ Systems Engineering Breakdown; Heritage

♦ Systems Engineering Breakdown
♦ Systems Engineering Breakdown; Heritage
♦ Design Review Weakness; Heritage
♦ Systems Engineering Breakdown
Gold Rule (1.11):

All use of heritage flight hardware shall be fully qualified and verified for use in its new application. This qualification shall take into consideration necessary design modifications, changes to expected environments, and differences in operational use.

Here is a New Gold Rule currently in review:

Do not qualify by similarity - use the traditional verification methods of test, analysis, inspection, and demonstration instead of similarity.
System Test and Evaluation Team

- Systems Engineering
  - Test requirements & evaluation

- Design Engineering
  - Test measurements
  - Test architecture
  - Test equipment requirements

- Test Engineering
  - Test planning
  - Test conduct & analysis
Verification and Validation Definitions

♦ **Verifying requirements:**
  • Proving that each requirement has been satisfied. Verification can be done by logical argument, inspection, modeling, simulation, analysis, expert review, test or demonstration. The primary methods, and those that we will discuss are test, demonstration, analysis and inspection.

♦ **Validating requirements** - Ensuring that:
  1) the set of requirements is correct, complete, and consistent,
  2) a model can be created that satisfies the requirements, and
  3) a real-world solution can be built and tested to prove that it satisfies the requirements.

♦ **Verifying a system:** Building the *system right*: ensuring that the system complies with the system requirements and conforms to its design.

♦ **Validating a system:** Building the *right system*: making sure that the system does what it is supposed to do in its intended environment. Validation determines the correctness and completeness of the end product, and ensures that the system will satisfy the actual needs of the stakeholders.
Data Flow Test Example

Example of end-to-end data flow for a scientific satellite mission

Exploration Systems Engineering: Verification Module
Test Facilities at Goddard Space Flight Center

General Information on GSFC environmental test engineering and integration:
♦ http://mscweb.gsfc.nasa.gov/549web/

Structural Dynamics Test Facilities (pictures & information)
♦ http://mscweb.gsfc.nasa.gov/549web/5492web/5492Pages/Facilities.htm

Electromagnetic Test Facilities (pictures & information)
♦ http://mscweb.gsfc.nasa.gov/549web/5493web/EMCFacilities.htm

Space Simulation Test Facilities (pictures & information)
♦ http://mscweb.gsfc.nasa.gov/549web/5494web/facility/faclayout.htm
Baseline Test Program for Flight System
Considerations for Reducing Integration and Test Time

♦ Easily verifiable requirements.
♦ Clear identification of the system level for each requirement to be evaluated
♦ Interface definition.
♦ Peer walkthroughs.
♦ Models and simulations.
♦ Robust design to component parameter variation, manufacturing process
♦ Robust inputs, targets outputs.
♦ Commonality, standardization.
♦ Simplicity.
♦ Testability.
♦ Reliability.
♦ Maintainability.
♦ Test equipment and facilities availability.
♦ Independence of components.
♦ Hardware emulator for untested software; tested software for untested hardware.
♦ Modular, bottom-up testing.
♦ Understanding of the critical path.
♦ Test plan and test procedures ready.
System Inheritance Review Topics

Description and prior history:
♦ Where inherited item was developed, to what requirements, workmanship issues, and condition.
♦ Original design, if available
♦ Performance history.
♦ Failure history and failure trends.
♦ Testing performed and results, analyses performed in lieu of test, and waivers for noncompliance
♦ Problem/failure report (PFR) system used, summary of all PFRs and red flag PFRs, waivers for noncompliance, and adequacy of PRF closures.

Intended application in the target project:
♦ Level of redundancy in application.
♦ Single-point failure philosophy
♦ Reliability analysis results and extent of independent review of these results.

Compatibility with project requirements:
♦ Design, qualification, and environmental requirements.
♦ Extent of changes required for project use.
♦ Parts classification, parts list of inherited hardware or design, parts specifications for parts used, non standard parts used, nonstandard parts authorization requests, and waivers.
♦ Operating system interfaces.
♦ Programming language
♦ Compatibility with host machine
♦ Support from provider
♦ Operating environment
♦ Configuration control: design compared to “as built,” change control requirement, when begun, waivers.
♦ Design changes made since qualification, and changes made or planned since last flown.
Spacecraft Environments

Research and know the environments in which your spacecraft must survive.

♦ Launch environment
  • Is your spacecraft manifested on a designated launch vehicle?
  • Vibration, noise, g-loads, aerodynamic loads, transition to vacuum, etc.

♦ Space environment
  • Is your spacecraft flying beyond the Van Allen belts or in LEO/GEO?
  • Hard vacuum, radiation, temperature extremes, orbital debris

♦ Planetary environment
  • Is your vehicle entering a planetary atmosphere?
  • Entry aerodynamics and the accompanying loads and heating

♦ Planetary surface environment
  • Is your spacecraft landing on a planetary surface? Moon, Mars, asteroid?
  • Gravity levels, terrain, atmosphere, dust, temperature
When the Genesis spacecraft returned to Earth on September 8, 2004, the parachutes failed to deploy. The spacecraft plunged into the Utah desert at 200 mph and broke apart. The redundant sets of switches controlling parachute deployment failed to respond to reentry deceleration because both sets were installed backwards as specified in the Lockheed-Martin design.

Questions:
- What happened at the technical reviews?
- Were the “design-to” specifications and evidence supporting the design approach provided at PDR? Were they assessed?
- Were the detailed designs, supporting analyses and development test data provided at CDR? Were they assessed?
- Were verification data proving compliance with specifications provided at SAR? Were they assessed?
Genesis – September 8, 2004

- 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