AEROSPACE REPORT NO.
TOR-2010(8591)-6

# Test Like You Fly:
# Assessment and Implementation Process

January 18, 2010

Julia D. White
Enterprise Mission Assurance
Corporate Chief Engineering Office

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

AEROSPACE REPORT NO.
TOR-2010(8591)-6

# Test Like You Fly:
# Assessment and Implementation Process

January 18, 2010

Julia D. White
Enterprise Mission Assurance
Corporate Chief Engineering Office

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

# Test Like You Fly:
# Assessment and Implementation Process

Approved by:

Christine L. Stevens

Christine L. Stevens, Principal Director
Engineering Directorate
Engineering and Integration Division
Space Systems Group

William F. Tosney

William F. Tosney, Chief Engineer/
General Manager
Corporate Chief Engineer Office
Systems Planning and Engineering

## Foreword

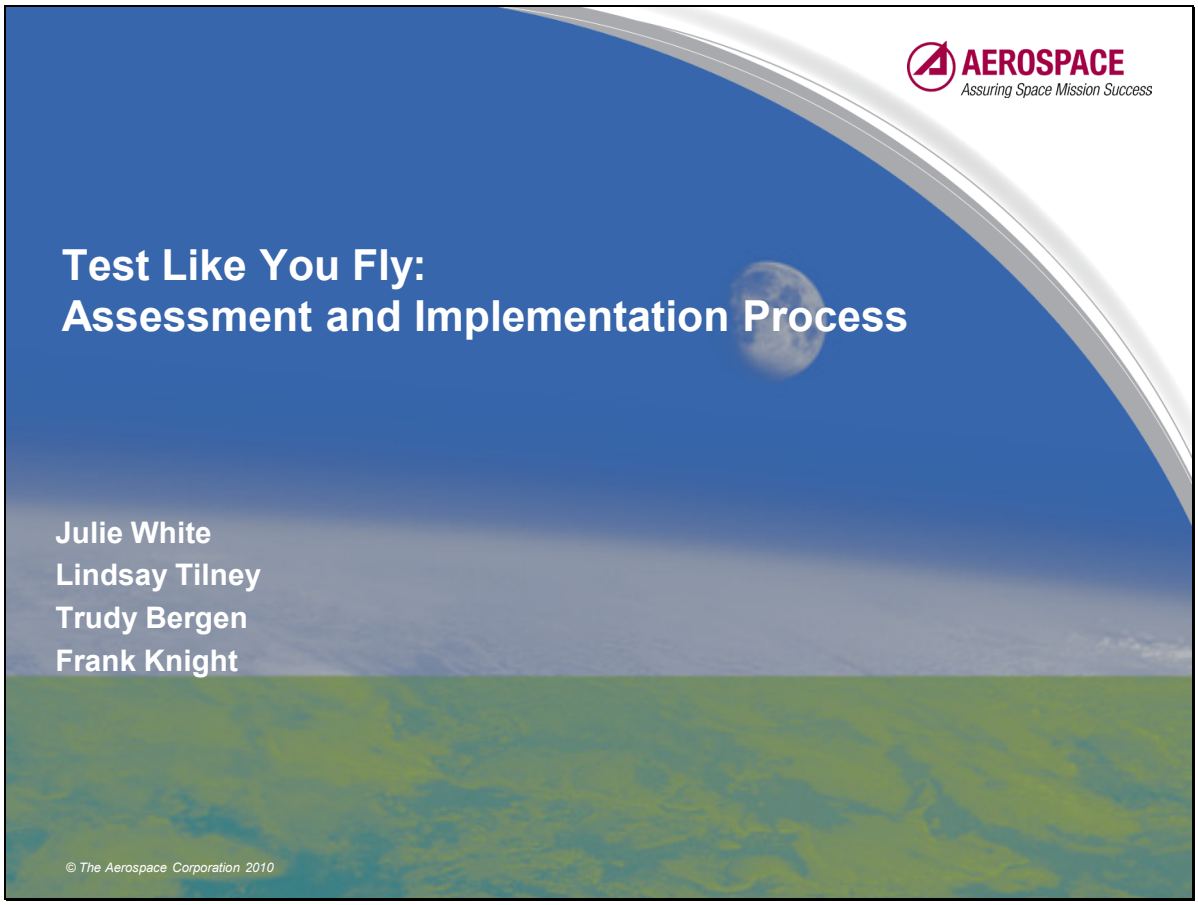
This TOR is a product of the 2008 Mission Assurance Improvement Workshop, which was held 13-15 May 2008 at Lockheed-Martin Deer Creek Facility, Denver, Colorado. The government/industry "Test Like You Fly" (TLYF) core team worked for six months prior to the 2008 workshop to identify a suitable product and to facilitate a brainstorming session with a wider community at the workshop. The original concept was to update a chapter on TLYF that was included in the 2006 *Space Vehicle Test and Evaluation Handbook* that had been written as an Aerospace Corporation Technical Report [TOR-2006(8546)-4591]. The workshop team created a list of various aspects that should be addressed by a TLYF assessment and execution process. After the workshop, it became apparent that it was necessary to create the outline of the process and its elements before the original chapter could be updated. Aerospace Corporation had created a "road show" in 2007 to help various groups, including the core team, understand the basic principles of TLYF. The core team provided comments and corrections to the road show. It was decided after the workshop to use this briefing as the basis for the final workshop product, complete with annotation. This product represents a substantial improvement to the description of TLYF principles and it describes the process that can be implemented to promote mission success.

**NOTE:** We will occasionally refer to "MIL-STD-1540" or "MIL-STD-1540E" in this document. This military standard ("Test Requirements for Launch, Upper-Stage, and Space Vehicles") is no longer an active standard. It has been updated and issued as an Aerospace Technical Operating Report (TOR) TR-2004(8583)-1 Rev. A, and as SMC-S-016(2008). As more engineers will be familiar with the old nomenclature than with the new report numbers, we will use the MIL-STD reference. If the reference is general, we will use MIL-STD-1540 to indicate something that has been in every version. We will refer to MIL-STD-1540E only when quoting directly from its text. However, we must emphasize that no edition of this standard addresses TLYF directly, and the tests specified therein are not LYF tests.

## Acknowledgment

The authors would particularly like to acknowledge the input and guidance provided by these participants in the Mission Assurance Improvement Workshop and subsequent interchanges: Dave Shelton and Dan Dimmock (LMSC); Ann Weichbrod (NGC); Brian Maxwell (Ball Aerospace); Pat Linder, Brian Schletz, and Cheryl Tsuchida (Boeing); Fred Smigiel, Roy Adams, Willy Miller, and Mathew Smith (ULA); Elizabeth Jones (Pratt Whitney Rocketdyne); Shelley Wells, Alice Shaw and Roger Talbot (LM IS&GS); Dave Kusnierkiewicz and Walter Mitnick (APL); Mark Graf (Integrity Apps); Roger Gibbs, Ben Jai, and Robin O'Brien (JPL); Michael Lovellette (NRL); Jon Hood (USAF); and Jason Feig, Bruce Arnheim, Barbara Braun, Bill Munley and Charles Wright (The Aerospace Corporation).

Slide 1




"Test Like You Fly" is a term that has progressed from being an undefined notion to an assessment and implementation process. This presentation will cover the following topics: the on-orbit failures that showed a need for more formality in applying TLYF principles; the philosophical underpinning for TLYF which makes it distinct from other forms of testing; the TLYF assessment process; what you need to know to be able to test "like you fly"; how to architect and design LYF tests; how to effectively implement TLYF at any program development phase; and how to determine and manage the risk of what cannot or will not be tested in a "like you fly" manner.

This approach includes a unique assessment and implementation process derived from mission failure lessons learned, and further developed by performing program assessments and workshops with government and industry communities of practice.

This formal approach is relatively new and several detailed facets are still evolving…. Hence, what follows is necessarily a work in progress.

Slide 2

## Expected Outcomes

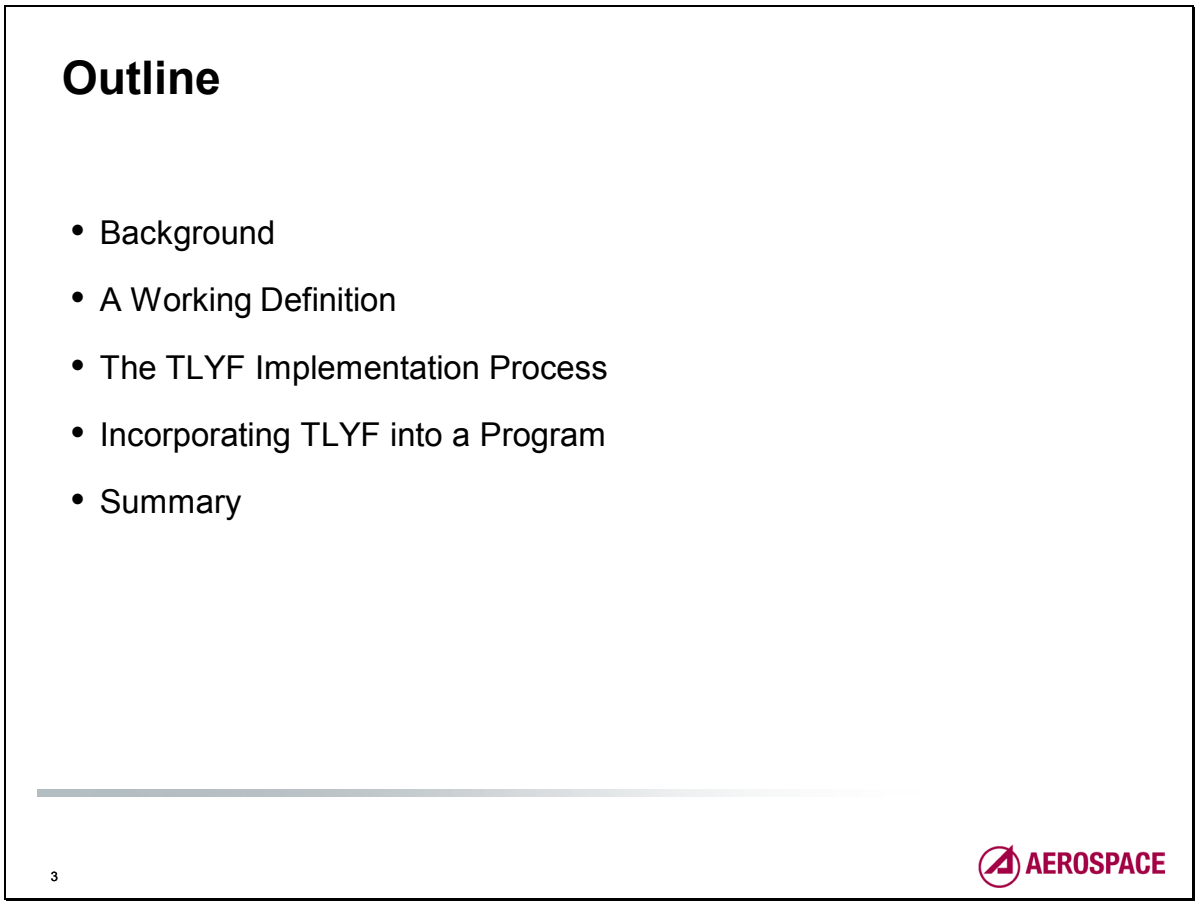
- Understand the value of applying the TLYF approach in the context of systems engineering and mission assurance
- Gain awareness of the distinctions between TLYF and other test techniques (i.e., Environmental, Qual, Performance, Functional, etc.)
- Describe the space community TLYF implementation principles
- Apply the TLYF process to space development projects and know when you're done
- Use the process to influence programmatic decisions
- Know how to participate in further refinement and application of the process





The purpose for this presentation is to provide a basis for applying the TLYF implementation process by highlighting relevant lessons learned, making distinctions between this process and other test processes, and detailing the basic steps including inputs and outputs.

Slide 3




The goals will be accomplished by providing the background leading up to the TLYF implementation process, defining a common definition and terminology usage, stepping through the details of the process which were derived from lessons learned, and lastly, recommending ways to incorporate the approach into a program.

Slide 4

## Assumptions, Caveats, Considerations

- Process developed primarily for low volume manufacturing numbers of free-flying, unmanned space vehicles
  - *Principles should be generic for other mission types*
  - *Applies to ground, space, and system of systems*
- Process described here assumes incorporating TLYF from beginning of the Acquisition life cycle
- How to add TLYF to programs already under contract will be addressed after process description
- TLYF is a team sport
  - *To get it right requires mission designers, systems engineers, operations personnel, flight hardware and software engineers, ground control hardware and software engineers, etc.*
- Words matter
  - *Common TLYF lexicon*

**TLYF is a work in progress**

4

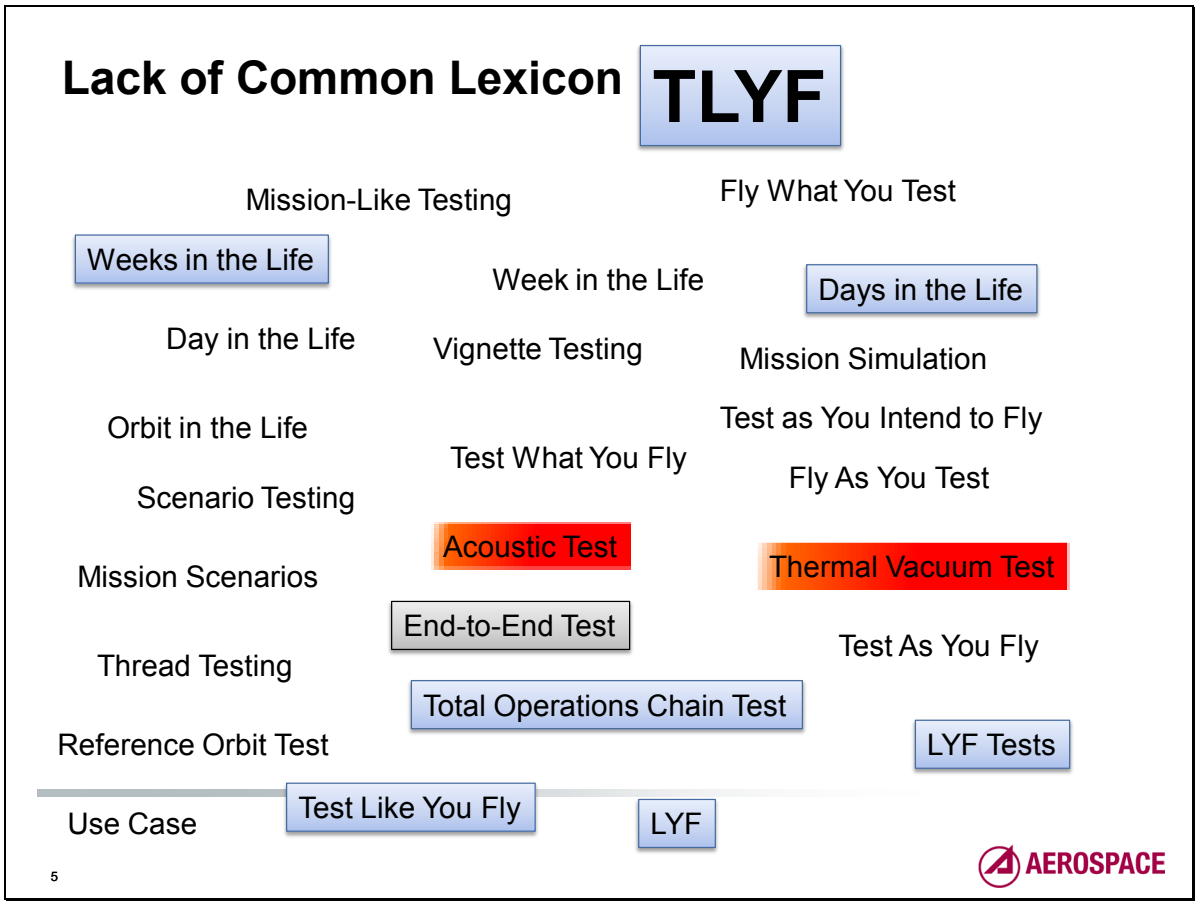
AEROSPACE

This approach is primarily focused on new developments. So, the walkthrough process assumes entering at the beginning of the program development. A few slides at the end will address applying the approach at various instances of the Acquisition Lifecycle.

In defining the TLYF approach an implementation process reveals that the topic is broader than "test." The TLYF approach has implications for acquisition strategy, interactive product development, requirements definition, systems engineering, fault analysis, and risk management.

In most sections detailed descriptions will not be within the scope of these charts, so only summaries of the implications will be included.

Slide 5




The lack of standardization implies that the implementation of *TLYF* is highly dependant on what it means, and doesn't mean, to the people involved locally. A properly implemented *TLYF* plan requires the participation of payload, subsystem, and operations specialists, who may not normally be associated with integrated vehicle testing. Consequently, the local interpretation of *TLYF* depends upon the individuals designing the tests. The statement that a program is using *TLYF* is insufficient without investigation of exactly how it is being implemented. A *TLYF* assessment is needed to do this investigation.

TLYF is highly dependent on what the phrase means, and does not mean, to the people involved. In this presentation the usage of terms has been narrowed down to “TLYF,” “LYF Tests,” “Total Operations Chain Test,” and “LYF.” These terms apply directly to the process herein described.

Because of the lack of a common lexicon, the meaning of terms that are applied to the process may be misrepresented. Most missions being launched in this era are complex enough to warrant days (something longer than a physical 24-hour sidereal day), if not weeks, to adequately exercise all mission phases.

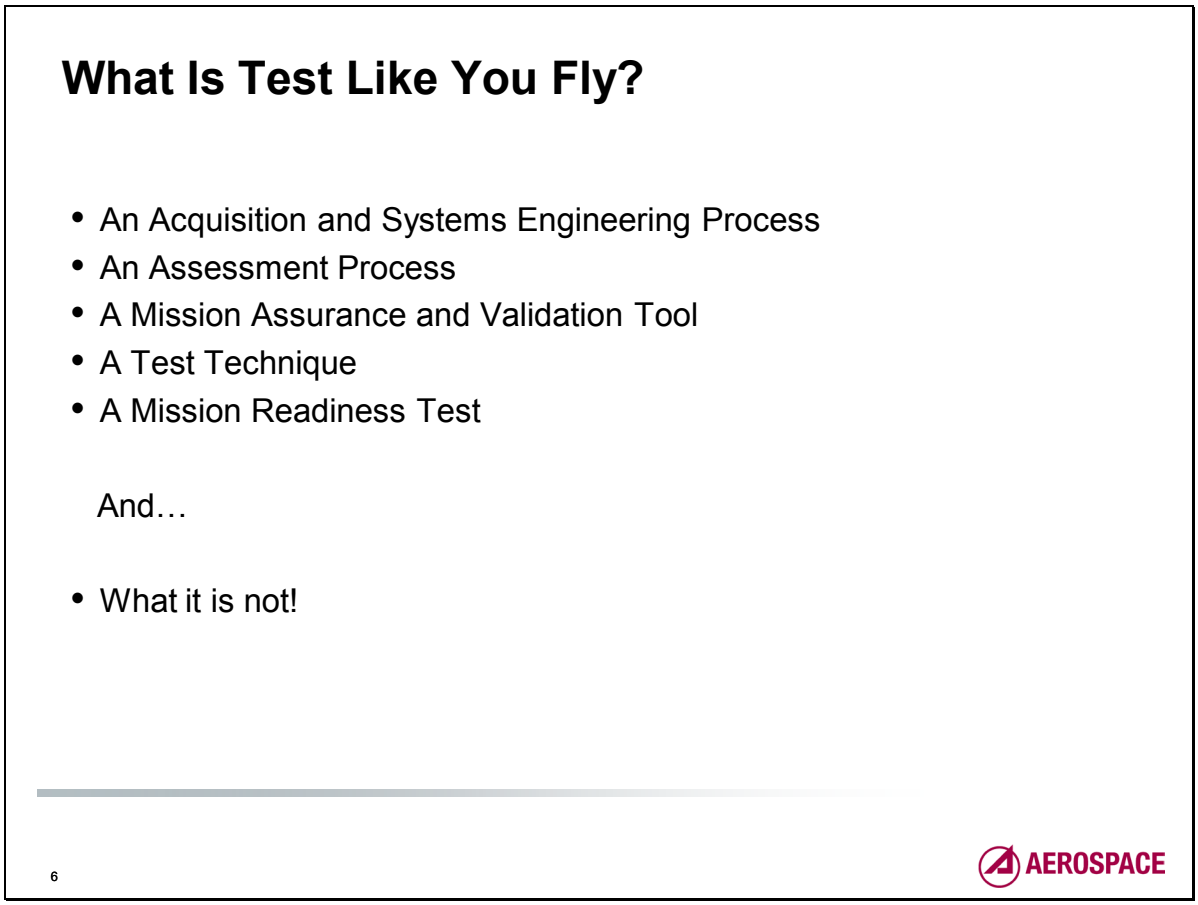
Terms need to be well understood and defined, e.g., a misuse of the term “days in the life” to mean only 6 hours is not a true representation of what is meant by “days in the life,” which would consist of a test duration of at least 24, if not many more hours. “Test as You Fly” is another phrase that mistakenly may mean test “while” you’re flying which is not the intent discussed herein.

Many of these terms will be defined later in the presentation.

We specifically are not including environmental tests defined in Mil STD-1540 (e.g., acoustic, thermal vacuum tests). These tests have other objectives; however, there may be opportunities to overlay them with LYF tests. This will be discussed later in the presentation as well.

Of the many terms that may be associated with the "Test Like You Fly" concept, those highlighted in blue will be used throughout the rest of this presentation. An End-to-End Test may or may not be a "like you fly" test, depending on the test objectives, hence, its gray color. The two tests highlighted in red – acoustic and thermal-vacuum – are essential environmental tests whose objectives are not related to mission demonstration. They are not intrinsically "like you fly" tests, and henceforth will not be included as such in this discussion, other than some recommendations and observations derived from the TLYF process.

Slide 6




TLYF is an approach that provides a unique assessment process that focuses on determining the "mission-related" or "like you fly" risks associated with potential flaws in our space systems. It encompasses much more than "test."

TLYF can be any of the following:

- A systems engineering methodology that focuses on more than verifying requirements, but focuses on the validation of a system's ability to perform its mission.
- A process to assess the mission concepts for testability and to assess the risk for those concepts that are not readily testable.
- A mission assurance mission validation tool to ensure that the acquired systems can accomplish the intended mission.
- A test technique for mission operability at all levels of assembly. This has an "end-to-end" aspect, meaning that it crosses interface boundaries, even if the "ends" aren't very far apart. Ends are truly the ultimate ends during the total operations chain test (TOCT), but are "brought in" for early validation of segments and lower levels of assembly.
- A specific readiness test: total operations chain (space + ground) days-in-the-life (DITL) / weeks in the life (WITL) operability test.

What TLYF is not will be discussed further, as it is essential to distinguish it from other processes, validation tools, and tests.

Slide 7

## Acquisition and Systems Engineering Process

- Acquisition considerations include
  - *Setting the risk level for program*
  - *Insuring schedule and deliverable coordination of mission operations, system design, and test planning development*
  - *Doing buy/make decisions that will inform RFP development*
- System Engineering considerations include
  - *Critical Fault Analysis*
  - *Risk Management*

***TLYF has a broader context than just "test"***

7

AEROSPACE

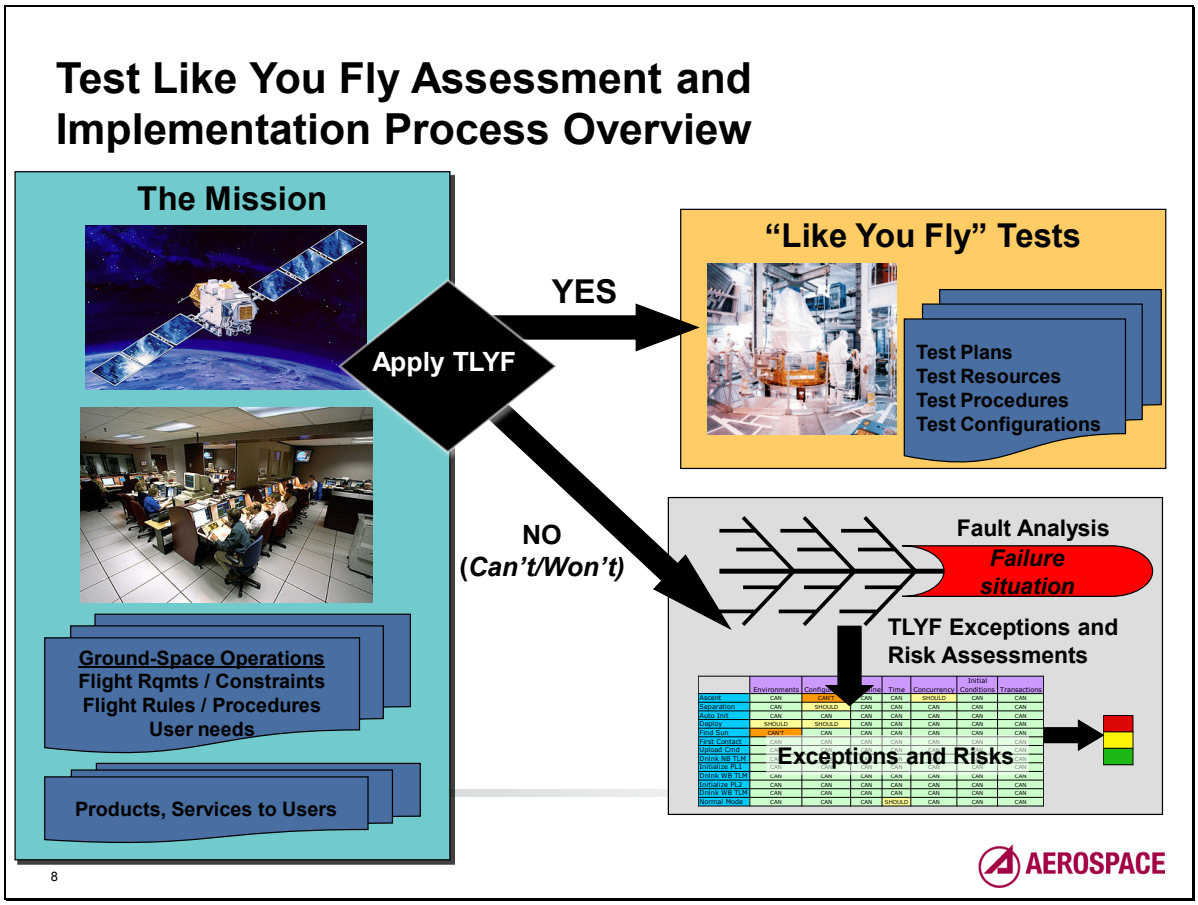
One of the results of defining the TLYF implementation approach is the revelation that the topic is broader than "test." The approach has implications for acquisition strategy, interactive product development, requirements definition, systems engineering, fault analysis, and risk management. As the detailed descriptions of these are not within the scope of this presentation, only a summary of the implications for each area will be included.

Test Like You Fly is a principle that goes beyond the discipline of "test." It provides a basis for acquiring and verifying a given system. It promotes a "mission centric" viewpoint for verifying and validating space systems. This can be incorporated early in the acquisition process.

Given that design decisions affect operations, and operations limitations have implications for design, and both have implications for test in general and TLYF in particular, this is an interaction that should be accounted for in the acquisition strategy.

The system engineering methodology instructs program managers to focus on verifying requirements. Requirements are primarily written in terms of system design and not system mission operability. This methodology has failed to emphasize the capability of test as a fundamental way to find flaws in the actual system that would preclude its ability to perform the mission. All systems, hardware, and software will have defects. It is vitally important to find what doesn't perform as expected and to understand the reasons for this anomalous behavior, especially where such defects can degrade, cripple, or end a mission. TLYF is a perceptive way to uncover such defects. Being able to demonstrate that a mission can be flown successfully is fundamentally different than demonstrating that a vehicle meets requirements. The risk of failing to TLYF can be severe.

Slide 8




Before anyone can "test like you fly," it is necessary to know how the mission will be flown. A process to assess the mission concepts for testability flows from that knowledge. The process is centered around a series of questions: What is feasible and practical to test? What needs to be available (documentation, hardware, software, procedures, trained personnel) to conduct feasible, practical tests in a flight-like way?

Like You Fly testing is driven by mission operations concepts, flight constraints, flight conditions, and mission considerations. It has an "operability" aspect and an "end-to-end" aspect, even if the ends aren't very far apart.

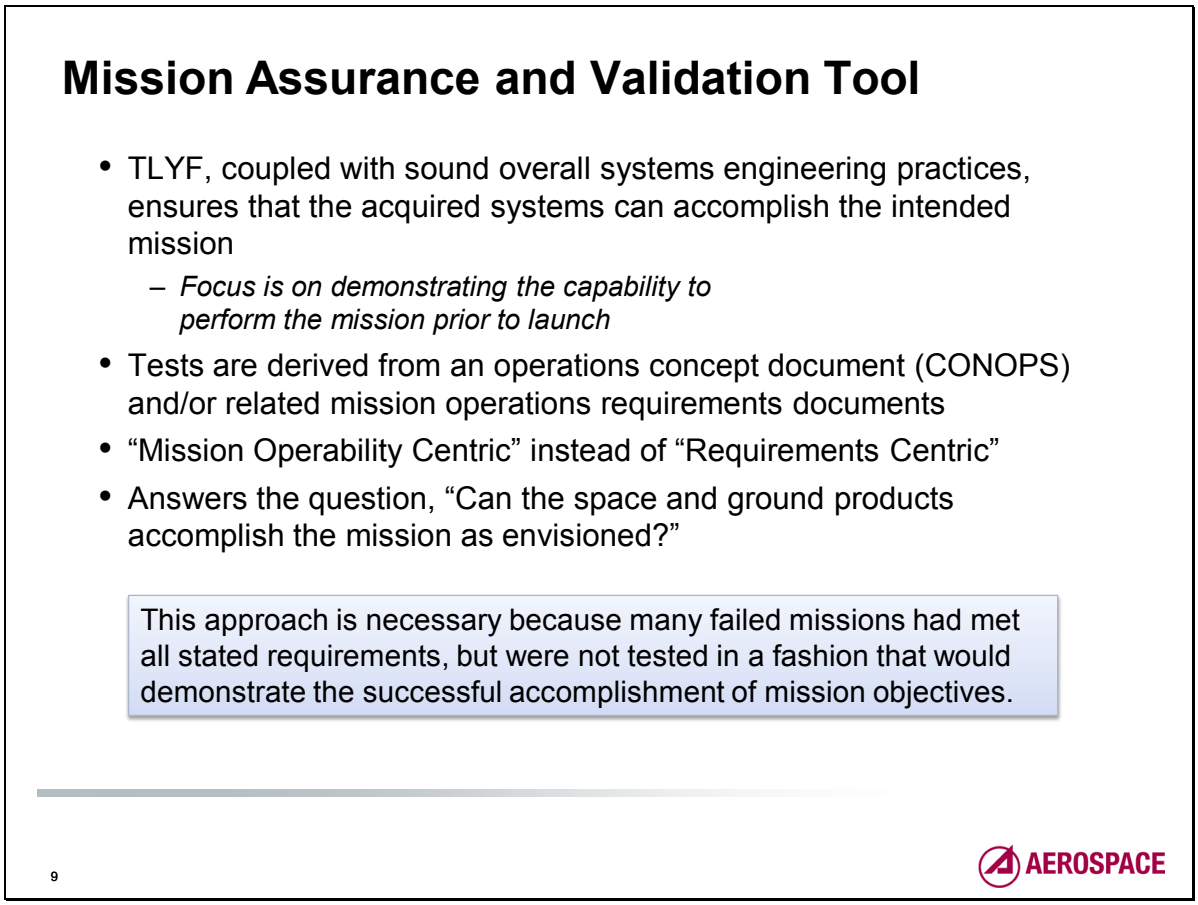
The prime "like you fly" characteristics are those in the time domain: continuous clock, timing, duration, order/sequence of events, including an appropriate set of initial conditions, a set of time-ordered events that include transactions and interactions among the elements between and at the ends, and any and all mission characteristics are applied (where possible).

A primary obstacle to executing flight-like tests is that there are many attributes of space flight that are not possible to re-create or adequately emulate in a pre-launch test. Rather than acknowledge that a test is not feasible or practical and leave it at that, it is necessary to assess the risk for those attributes that are not readily testable.

When we can't do the obvious test, which is often impractical or impossible, we run the risk of failing to detect mission-critical flaws. When we have to abridge a test or substitute non-flight articles or aspects to be able to run a reasonable approximation of flight, we also run the risk of missing flaws.

In the absence of the ability to run a perceptive test, the TLYF assessment process includes an evaluation of these missing aspects to determine what can go wrong, and whether undetected flaws can contribute to a mission critical situation. If such a potential flaw exists, it must be identified by some other means and mitigated accordingly. Hence, the TLYF assessment process accounts for the risk of not being able to test in a flight-like manner by evaluating TLYF exceptions.

Slide 9




TLYF can be considered a mission assurance mission validation tool, primarily because the "like you fly" tests are derived from an operations concept document (CONOPS) and/or related mission operations requirements documents, rather than being derived from a systems requirements verification approach. The knowledge concerning what the mission is and how it is to be flown is typically documented in the CONOPS and other mission description documents that frequently are not captured in a requirements verification matrix. Specific operational requirements documents that may be used as communication tool between acquisition and operations organizations are also not likely to be represented in formal verification processes. These are the applicable references for assuring mission success.

An initial CONOPS may be very broad in its descriptions. The process of assessing our ability to perform LYF tests is iterative. The initial CONOPS will either need to be updated to be as comprehensive and complete at each point in the development process where the TLYF assessment is reviewed, or follow-on detailed documentation for mission processes will need to be produced.

This approach asks the question: Can the space and ground products accomplish the mission as envisioned? This approach is necessary because many failed missions had met all stated requirements, but were not tested in a fashion that would demonstrate the successful accomplishment of mission objectives. Flaws in properly identifying, decomposing, and communicating requirements are a source of error, especially where those requirements do not adequately account for the operational environments and other conditions associated with flight.

Slide 10

## An Assessment Process

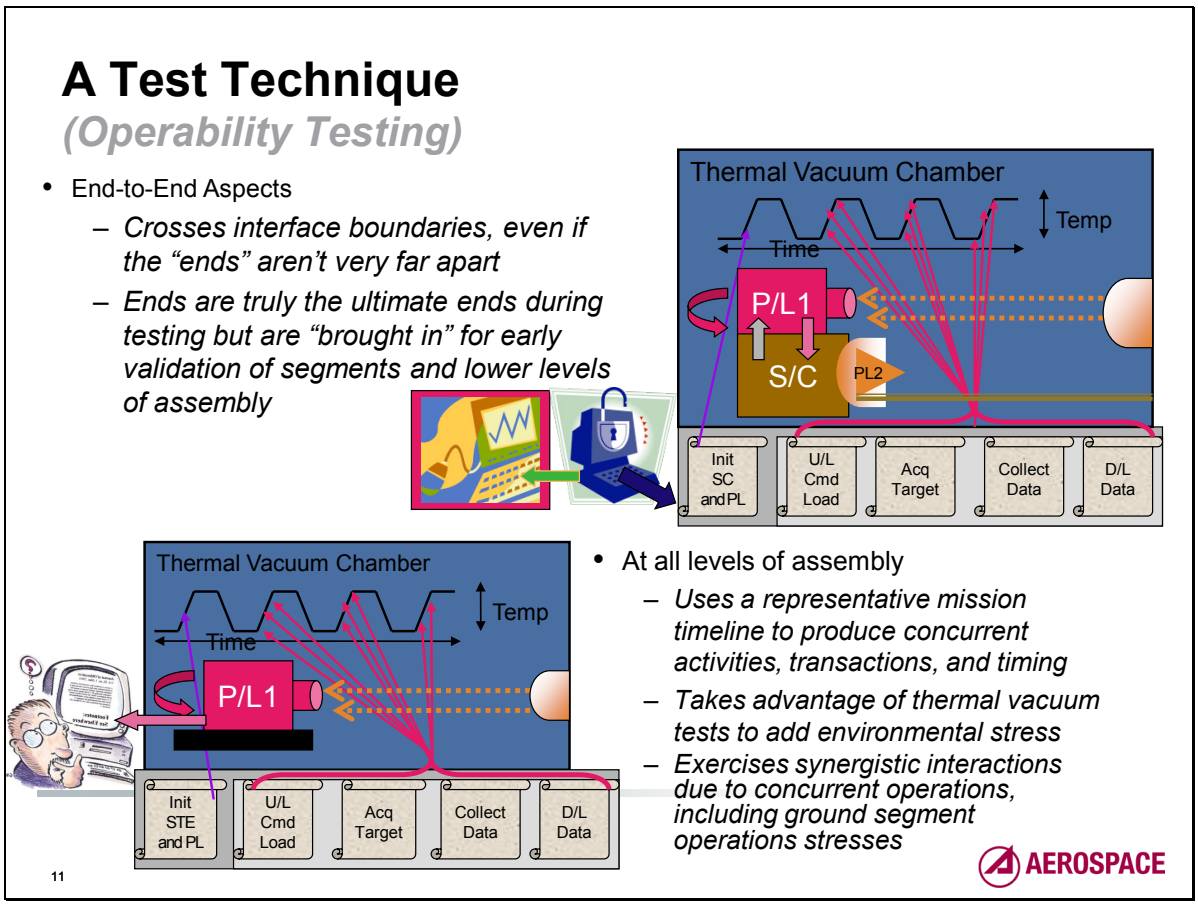
- A process to assess the mission concepts for testability and to assess the risk for those concepts that are not readily testable
  - *Be able to determine exit criteria, knowing when you're done*
- Establishes guidelines for implementing TLYF
  - *Describes, in usable detail, a process that can be used by USG space system acquisition personnel, their contractors, and independent reviewers to assess:*
    - The degree to which a test program can and does incorporate TLYF principles
    - The risk exposure of not testing like you fly
  - *Defines and develops a TLYF evaluation process from basic engineering science principles and lessons learned*
  - *Provides generic strategies and techniques that can be used as a basis for discussion in each mission area and project*

10

AEROSPACE

A primary obstacle to executing flight-like tests is that there are many attributes of space flight that are not possible to re-create or adequately emulate in a pre-launch test. Rather than acknowledge that a test is not feasible or practical and leave it at that, it is necessary to assess the risk for those attributes that are not readily testable. Operability tests are very perceptive at discovering several classes of flaws, including hardware/software timing issues, memory leaks, data errors, and effect of combined environments on processors. Note, many of these may manifest as intermittent errors, and only under conditions of full operational loads and long duration runs.

Slide 11



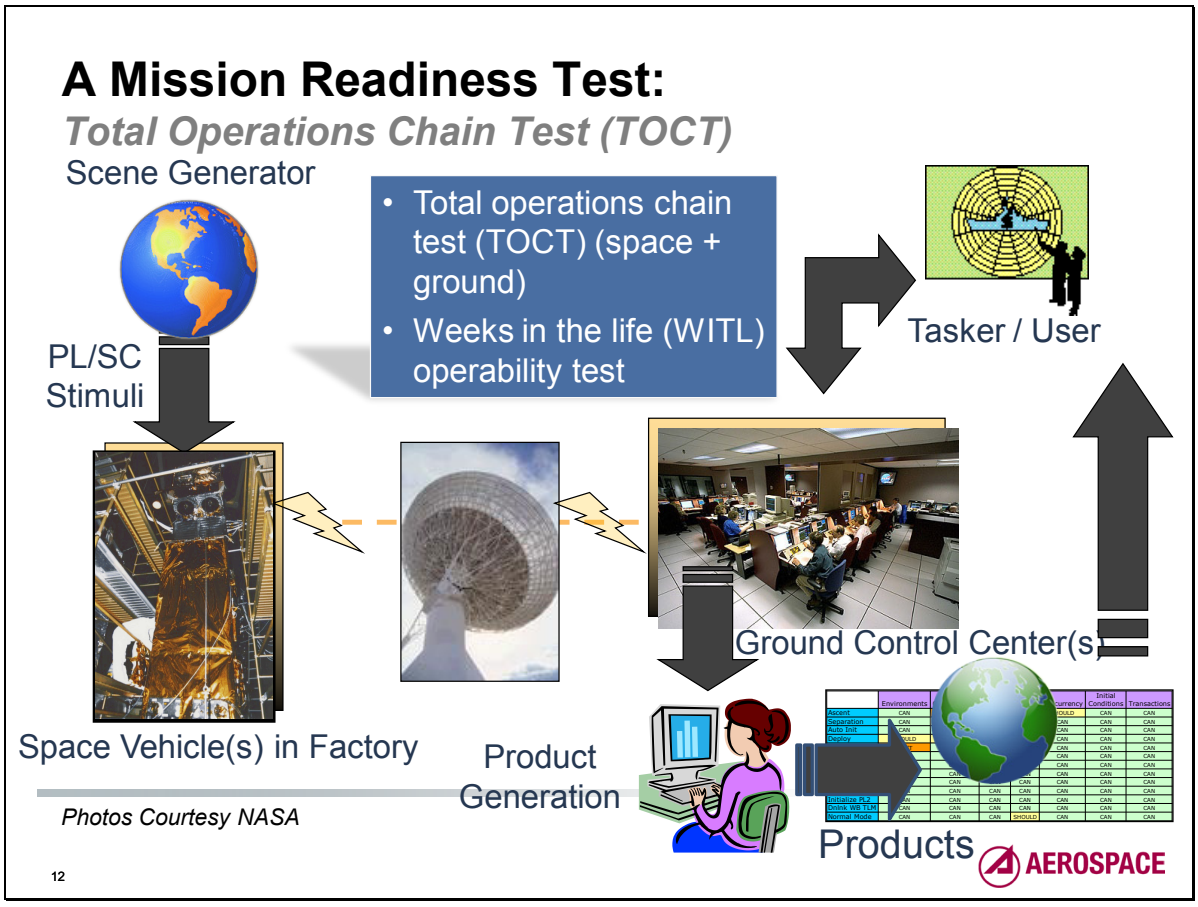

TLYF as a test technique for mission operability results in specific tests, different from simple functional or performance tests, designed to show that the item or system is capable of performing its tasks in the context of mission conditions and timelines. "Mission conditions" can be aspects of the space environment (e.g., radiation, thermal, and vacuum), but there are many more applicable attributes (e.g., commanding, telemetry, configuration, and operations environment) as will be detailed later.

Much of our established testing based on test specifications (e.g., MIL-STD-1540) ignores the time component, which is a vital factor in executing a mission. TLYF tests must show the ability to properly transition from one activity to the next, to sustain duty-cycle driven activities, to demonstrate timing interactions between asynchronous activities, and allow for error growth and discovery in software execution (e.g., counting errors, buffer overflow, and clock roll-over).

At all levels of assembly, use a realistic mission timeline to include all first time-, mission critical-, and mission objective- events, and sustained activities appropriate for the level of assembly and in context of that assembly's contribution to the mission. Strive for realism in environments with operational stresses (power, throughput, etc.) to better characterize performance. Use multiple, synergistic environments where possible. Exercise synergistic interactions due to concurrent operations, including ground segment operations stresses.

A propulsion system, for example, can only be tested in a very limited way once integrated into a space vehicle, due to facility and contamination issues. Mission conditions and characteristics need to be assessed for which of these need to be applied at the lower levels of assembly to be able to expose flaws that are only able to be seen under those conditions.

Slide 12




TLYF is ultimately a specific readiness test of the total operations chain, sometimes known as an end-to-end (space + ground) days-in-the-life (DITL) / weeks in the life (WITL) mission operability test. We will call this the "total operations chain test" (TOCT). A notional concept of the total operations chain test is shown in the figure above. The chain has inputs from payload and spacecraft stimuli. Some missions are taskable and will have inputs from tasking organizations. Outputs from the chain will include either mission products (e.g., images and data) or mission services (e.g., communications, navigation).

The TOCT should reflect the architecture of the mission, per mission phase, as defined in the concept of operations. It necessarily includes the SV in the factory, under control of ground station assets, being flown in the flight-like manner to the extent feasible. The TOCT is the bridge between the SV in the factory controlled from the ground station, and the flight CONOPS that should explain how the mission would be flown. Experience from integration and test organizations that require such end-to-end testing is that this test finds defects that cannot be detected in any previous testing, including full electrical, functional, and performance testing.

The TOCT may be extended to demonstrate a specific mission duration, whether it be a day, days, or weeks in the life of the system.

The TOCT is intended as time-driven end-to-end test and is not intended to be a substitute for dynamic (closed-loop) tests that may only be perceptive at lower levels of integration, or that need certain special test equipment/simulations (as an adjunct to—or in lieu of—flight equipment) to be accurate.

This is a test already required by NASA GSFC and the European Space Agency (ESA). It is as close to “flying the mission pre-launch” as is possible. It is an opportunity to bring together all the hardware, software, processes, tools and personnel involved in executing the mission to expose major defects between elements and flaws preventing smooth operations between the ground and space elements. This is a natural follow-on to limited functional end-to-end tests, such as RF compatibility.

Slide 13

## TLYF for Dummies

"Test Like You Fly" is a pre-launch systems engineering process that translates mission operations concepts into perceptive operability tests and assesses the risk of missing mission-critical flaws when it is not feasible to do those tests or adequately represent key mission characteristics while executing such a test.

13

AEROSPACE

A simplified definition is also provided which highlights the necessary aspects of TLYF:

- Tests are conducted before the system flies
- Mission Concepts are used to define perceptive tests
- Risks are uncovered based on a "mission critical" perspective of missing flaws

Slide 14

## TLYF: Working Definition*

- TLYF is a pre-launch systems engineering approach that examines ***all applicable mission characteristics*** and determines the **fullest practical extent** to which those characteristics can be applied in testing.
  - *"**All applicable mission characteristics**" are concurrent attributes including, but not limited to, hardware and software configuration per mission phase or activity, external environments, internal induced environments, automated flight sequences, commanded operations, activity order and timing, up/downlinked telemetry, data product generation, signal services, mission planning, and end-user evaluation.*
  - *The "**fullest practical extent**" identifies the physical and engineering limitations, and balances what can be done in a flight-like manner with acceptable and understood risk and program constraints. The test article can be anything from a complex component, through all levels of integration, up to and including all space and operational software and systems involved in conducting the mission, but should ultimately be the final flight article.*

***TLYF doesn't start with test***

14

* Evolved from Space Vehicle Test and Evaluation Handbook, Chapter 33, Julia White and Charles Wright, The Aerospace Corporation, 2006

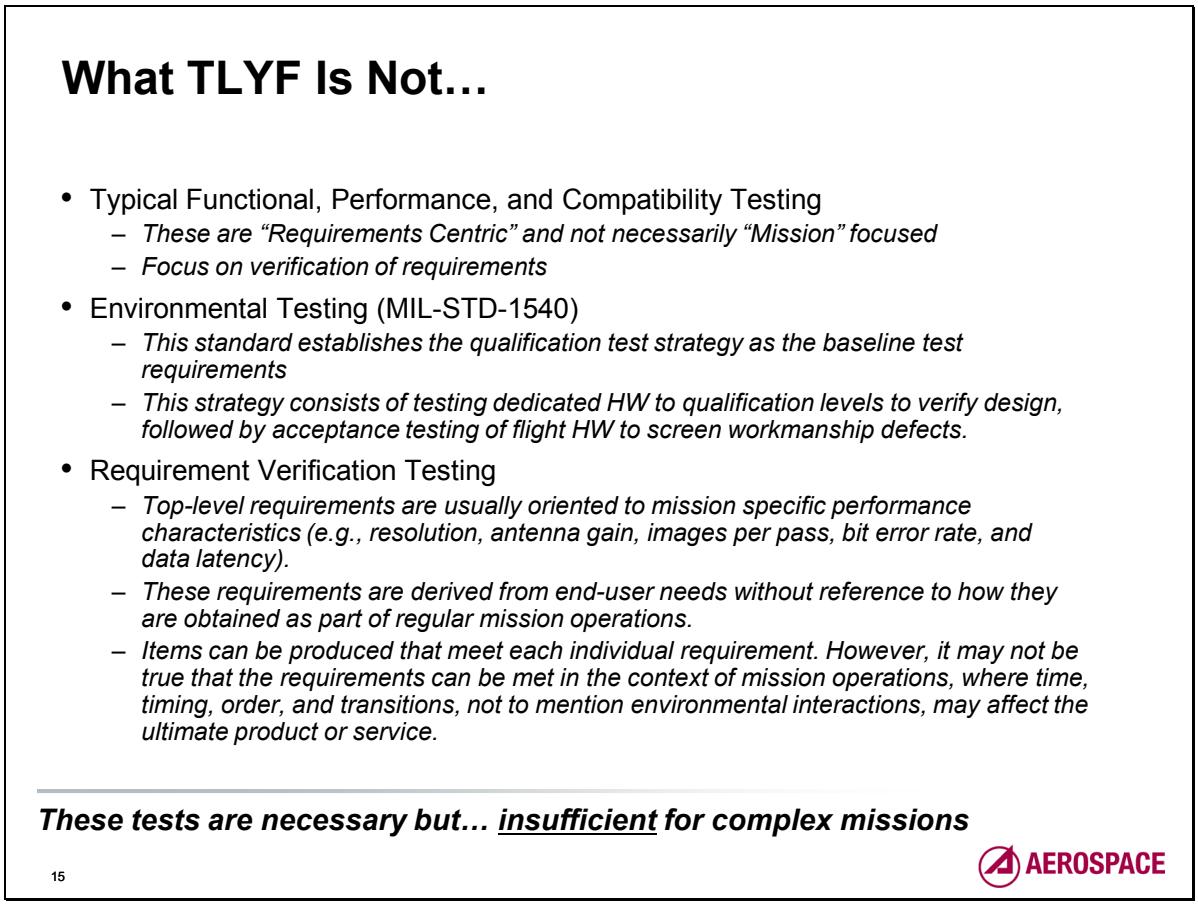
AEROSPACE

As mentioned earlier, the phrase "Test Like You Fly" can take on several meanings depending on the frame of reference or experience. To minimize confusion we have provided a working definition accompanied by clarification of terms.

Another problem with terminology is that there are other phrases and concepts that are commonly thought to be associated with TLYF. Without getting into fundamental philosophy, we will use this phrase to mean what is set forth in this presentation, and we will make a distinction between TLYF and other forms of testing that may be precursors, adjuncts to, or completely independent of LYF tests.

To ensure a common terminology, this working definition of "test like you fly" is recommended.

Slide 15




It may be tempting to think that every test that is connected to or derived from mission concepts or requirements is necessarily "like you fly." The processes described here are derived from specific lessons that follow a different approach than lessons already incorporated into existing test specifications and standards. We are intentionally separating tests that are meant to verify design and performance requirements from operational requirements verification and operability validation. This means that we don't include in our TLYF processes those tests (1) whose objectives include a determination of margin, (2) whose approach is determined by qualification/protocol/acceptance levels and related guidance, or (3) whose relevance is assessed by evaluating form/fit/function.

Requirements verification tests are necessary, but not sufficient for complex payloads, spacecraft, systems, and missions. The lessons from a number of catastrophic failures have taught us that it is necessary to include tests that are "mission operations centric," where the focus is to demonstrate pre-launch the capability of an integrated items or system to perform the mission. Demonstrating that hardware survives an environment, although a necessary prerequisite, is not the same thing as showing that the integrated hardware/software/processes/procedures work.

These "other tests" that are not necessarily themselves LYF include, but are not limited to: functional (low level), performance, calibration, environmental, qualification, compatibility, interface, and thread. These are each valuable and perceptive to uncovering specific flaws and effects, but they are not generally LYF unless they are specifically designed to be LYF. Functional and thread tests can be considered, along with scenario tests, as lower level precursors to timeline and mission phase testing.

Slide 16

## How Does a LYF Test Differ from Other Tests?

- LYF tests are not directed at requirements verification – unless the requirement is specifically concerned with operability under mission conditions
  - *Requirements verification is necessary, but not sufficient*
- Pieces and parts versus an integrated system
  - *Showing that every individual item "works" is not the same as showing that all items work together*
- LYF tests are not driven by the test design principle of varying a single independent variable to isolate dependencies on that variable

16

AEROSPACE

Functional and performance tests, run from electrical ground support equipment (EGSE), are not TLYF activities, but they necessarily precede TLYF activities. "We send flight commands. We get flight telemetry. What else is there?" This is a common reaction among spacecraft test engineers. This is because test engineers are not familiar with how mission operations are done. It is also because they make an assumption about the equivalence of test equipment and ground control equipment. Commands sent to exercise each end item in a subsystem or unit, whether by logical order or alphabetical order, will verify the expected response. However, this is nowhere near the method used to fly the mission. It simply isn't Like You Fly. During the mission, numerous and complex tasks are being performed in parallel all over the vehicle in a non-deterministic, asynchronous fashion.

MIL-STD-1540E defines functional testing as "testing against requirements that relate to *actions and activities* assigned to the item(s) under test." Functional testing, as generally expressed in satellite manufacture and test, involves sending commands to perform the functions of individual units or subsystems in a serial fashion, addressing one unit or subsystem at a time, and noting the responses. Functional testing answers the question, "Is this unit or subsystem performing its functions properly under these specific test boundary conditions?" Functional testing necessarily precedes *Test Like You Fly* activities. Functional testing is generally, however, not a *Test Like You Fly* activity. In our experience, the contractor may incorrectly offer functional testing as a *TLYF* activity.

Performance testing is defined, in MIL-STD-1540E, as "testing that is conducted against technical requirements that *quantify* the extent the requirement must be executed." A performance test provides *measurable and trendable* parameters. Performance testing also precedes *TLYF* activities, but is generally not a *TLYF* activity. Performance testing may also be incorrectly offered up as part of the

contractor's *TLYF* activities. Some performance tests may lend themselves to TLYF approaches. Performance tests done in a flight-like manner are the basis for "fly like you test."

Slide 17

## Basic Principles and Tenets of TLYF

- First:
  - *The system should never experience expected operations, environments, stresses or their combinations for the first time in flight*
- Second:
  - *Do only smart things with the space system*
- Third:
  - *TLYF is a **complement** to other forms of performance and functional testing, NOT a replacement for other perceptive testing (e.g., vibration testing with electronics powered and active)*
- Fourth:
  - *When you can't test like you fly - worry (or do risk management)*

***Murphy is alive and well and working overtime on your program!***

17

AEROSPACE

The TLYF approach focuses on reducing risk in key mission areas.

**First**:
The programmatic and physical limitations and constraints need to be considered upfront.

**Second**:
This approach should not drive you to purposely break flight HW. In other words, it should not lead you to expose the Flight HW to known damaging test configurations or environments. However, if the execution of a LYF test reveals a flaw that damages the HW unknowingly, from a TLYF perspective, this is viewed as a successful test, uncovering a flaw on orbit with detrimental effects.

**Third**:
We are not recommending that TLYF infiltrate every test conducted. We recognize the value of other tests and merely want to add another tool in ensuring mission success.

**Fourth**:
It is not sufficient to merely state "we can't test like we fly" and ignore the implications involved with that statement. It is necessary to account for the risks derived from not conducting LYF tests.

Slide 18

## Why We Want to Test Like You Fly

*Keep the Goal in Mind*

- Requirements verification is necessary, but not sufficient
  - *Verification under non-mission conditions (timeline, concurrency, etc.) with non-flight elements or an incomplete configuration or previous (pre-repair) configuration or without the last pre-flight software load **WILL** miss the errors/flaws/defects that **ONLY** occur under mission conditions*
- The goal is to have literal "like you fly" tests for as many flight and mission phases as practical
  - *We got here because of failures to do these kinds of tests*
- The goal is *not* to change environmental, performance, or calibration tests into "like you fly" tests
- We got here because of failure to account for the flaws we can't find directly by test

18

AEROSPACE

By focusing on requirements verification for space systems, many flaws and defects escaped the test floor. Lessons from post-launch mission failures since 1990 form the basis of the TLYF process.

Each anomaly occurred after liftoff on a space vehicle or launch vehicle that had its requirements, functionality, and performance verified prior to launch. These vehicles had passed their "requirements-centric" tests. When examined using the TLYF approach, the likelihood of encountering these anomalies may have decreased. Various violations of the approach allowed these anomalies to escape to the launch or mission phase. Unfortunately, most of these failures resulted in total loss of mission.

The goal of Test Like You Fly is to provide a complementary test approach that promotes literal "like you fly" tests for as many mission phases as are deemed necessary and critical.

It is not intended to change existing tests into "LYF" tests, unless it makes sense and is cost effective.

Based on mission failures over the past ten years, it seems alternate processes are needed to catch flaws and thus—the creation of the TLYF process.

Slide 19

## Failing to *Test Like You Fly*

### *Lessons Drive the Process*

- Post-mortem analyses of failed missions show consistent violations of the *Test Like You Fly* approach to be significant contributors to loss of mission

| VEHICLE | YEAR | MISSION CRITICAL ANOMALY ROOT CAUSE | TLYF VIOLATION | RESULT |
|---|---|---|---|---|
| Titan CT-2 Launch | 1990 | Miswiring prevented satellite separation; Ground test using non-flight software did not identify the problem. | Test What You Fly | Loss of Mission |
| ESEX Payload | 1999 | Exploded in space after leaking battery electrolyte caused short circuit; Bettery qualified in non-flight condition. | Test Like You Fly | Loss of Mission |
| Mars Polar Lander | 1999 | Faulty touchdown sensor logic caused vehicle to crash; Test not rerun with hardware and software after modification. | Test Like You Fly | Loss of Mission |
| Mars Climate Observer | 1999 | English-Metric units error crept into modified software; Being deemed non-critical, was never tested. | Test Like You Fly | Loss of Mission |
| WIRE | 1999 | Start-up transient in pyrocontroller caused premature telescope cover deployment allowing coolant to escape; GSE power supply hid the problem. | Test What You Fly | Loss of Mission |
| TERRIERS | 1999 | Torquer coil installed upside down; Hardware and software never tested together. | Test Like You Fly | Loss of Mission |
| Milstar 2-F1 Launch | 1999 | Improper filter coefficient loaded into flight software; No validation of filter constants actually flown. | Test What You Fly | Loss of Mission |
| Genesis Return Capsule | 2004 | Four deceleration switches installed backwards causing parachute failure; Never tested in flight configuration. | Test Like You Fly | Significant Loss of Science Product |

19

AEROSPACE

Here's a summary of mission critical failures and the mission critical anomaly root cause.

These data helped form aspects of the TLYF implementation process discussed herein. Each "step" has been created to mitigate the occurrence of such failures in the future.

The system engineering methodology tells us that we test to verify requirements. We also test to find flaws in the actual system to assure its ability to perform the mission. Functional and performance tests are the first opportunities to observe the integrated vehicle in action. All too often, functions and responses differ, in a negative way, from those anticipated. It is vitally important to find what doesn't perform as expected and to understand the reasons for this anomalous behavior. *TLFY* may be the only way to identify defects that would otherwise cripple, or prematurely end, the mission. True *Test Like You Fly* activities come from a "Mission Success" context. Being able to demonstrate that you can successfully fly the mission is fundamentally different than demonstrating your vehicle meets requirements. The risk of not testing *Like You Fly* can be severe, as the table shows.

One critical lesson derived from this table is that loss of mission failures occurred in spite of adherence to environmental testing. The root causes for these failures are not related in any way to environmental conditions. They are related to the way in which the mission is executed in various mission phases, thus highlighting the need for a different test perspective.

Slide 20

## Lessons from Titan CT-2: Know the Mission

*Assess Differences between Current and Previous Mission*

Payload separation error due to incorrect electrical wiring

Can you count to 2 if there's only 1?

- **Lesson**: Test What You Fly
  - *Heritage doesn't confirm changes and differences*
- **Lesson**: Test How You Fly
  - *Test across mode and phase transitions*

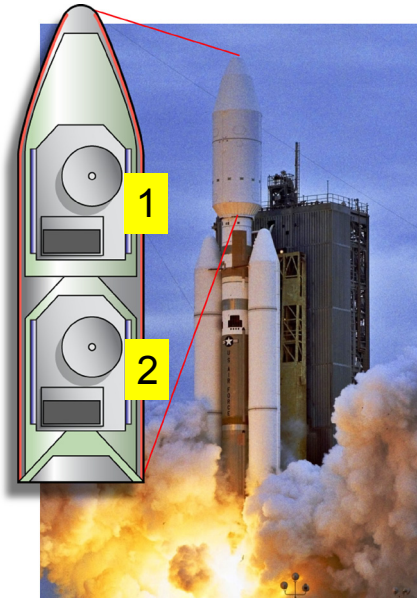



Photo Courtesy of NASA

***Loss of Mission***

20

AEROSPACE

The Titan CT-2 provides an excellent example about the need to look closely at each mission. This lesson involves a case where this launch vehicle mission was different from a previous mission. The prior mission (CT‑1) was configured for two payloads as shown in the diagram. CT-2 was configured for only one payload.

**Incident Summary**
On 03/14/90, a commercial Titan launch failed to deploy the Intelsat 603 payload. The failure was caused by miswiring, which was not caught on the ground due to a non-flight-like testing approach.

**Cause of Failure**
The 4-meter shroud was designed to accommodate two payloads, and the previous launch, CT-1, was a dual launch. However, only Intelsat 603 flew this time.

The draft Mission Specification had the separation commands sent to the "forward" position (Figure 1). An electrical design engineer redlined the commands to "aft" to simplify wiring. Unfortunately, this change was not incorporated in the final mission specification.

Not realizing that the informal redline had fallen through the cracks, the hardware group designed an incompatible harness. The drawings were released as a new baseline, making it difficult to detect crucial changes. Several systems engineering departments could have checked the compatibility of the final design to overall requirements, but none did—the key mission specification was developed by software engineers and was not placed under systems engineering's jurisdiction. As Norman

Augustine (CEO of Martin) said: “The only problem was that somewhere along the line, we had designed in an escape vent in our configuration control system.”

**Cause of Verification Escape**
The mistake was not discovered on the ground because the generic systems test activated both forward and aft positions, allowing the miswired ordnance verification unit to appear to be working.

**Manifestation of Failure**
As the payload was stuck with the second stage, the launch team released the satellite from the perigee kick motor—still attached to the launcher—to a low orbit. Eventually, a new perigee kick motor was brought in by the shuttle, making it possible to reboost Intelsat 603 to the intended orbit.

Slide 21

## Failing to *Test Like You Fly*

### *Down the Test Pyramid*

| Vehicle | Mission Critical Anomaly and Root Cause | TLYF Issue | Integration Level of Flaw Detectability | Applicable Flight Characteristics |
|---|---|---|---|---|
| Titan CT-2 | Failure to separate SV. Miswire/ numbering error for single payload. | How and What we fly | Integrated System | Timeline, sequence, configuration, command |
| Ariane V | Inertial Reference System disabled. "Dead code" inherited from Ariane IV. | What we fly | LV /SV /Ground<br>Subsystem | Sequence, end-to-end level, fault management |
| ESEX Arcjet | Battery explosion. "Heritage" battery and charging system not able to sustain unique charging scheme. | How we fly | Unit or Assembly | Duration |
| AV-009 | Wrong orbit. Engine fuel inlet valve did not close fully at end of first burn, resulting in overboard fuel leak during coast phase. | How we fly | Subassembly<br>Discrete Part | Duration, internal environment |

21

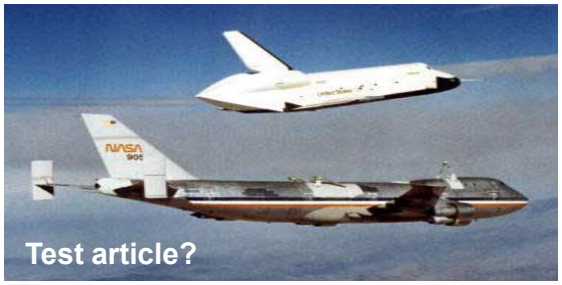
AEROSPACE

The failures that we looked at included lessons that indicate where in the development cycle one can begin to apply TLYF principles. The principle can be applied down to the lowest level of assembly. We will discuss the details and provide examples of this later in the presentation.

Slide 22

## Determining the Extent to Which TLYF Should Be Applied

- Is the project doing something brand new?
- Is the project using something "heritage" in a new design or application?
- Is the project doing something where other, non-LYF techniques have evolved to validate operability?




Courtesy of USAF Courtesy of NASA



22

AEROSPACE

When a system and mission are completely brand new (i.e., the shuttle program at its beginning stages), there is a need for more extensive incorporation of TLYF.

Heritage systems like Milstar 1 was for Milstar 2, are built by the same supplier and have similar design and concept of operations. However, a legacy system is a previous generation like Milstar is for AEHF.

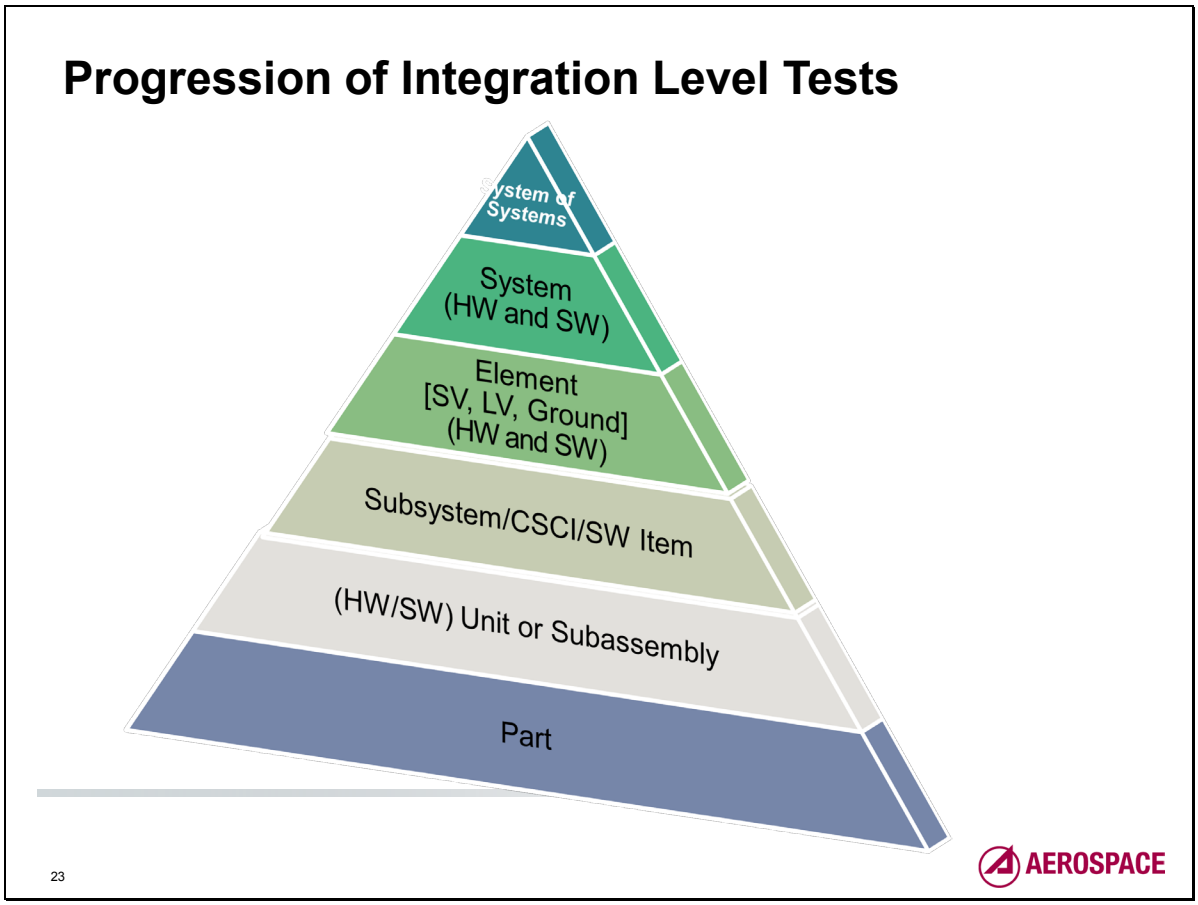
Missions that are evolved from legacy systems will require detailed planning upfront to allow for utilization of operational resources

Missions that are evolved from legacy (previous generation) systems and are expected to be backward compatible, have other LYF test needs that should be considered in the Pre-Systems Acquisition phase. Primary issues to be evaluated are:

(1) the extent to which the new system will need to be tested with legacy equipment (both space and ground), and

(2) how that can be accomplished with minimal or no mission impact.

Slide 23




Tests are performed at all levels of integration of the Hardware (HW) and Software (SW), ending with the absolute final version of a Space Vehicle in the factory with the operational HW, SW, dates, and procedures at the ground station.

**System of Systems**: A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole. (CJCSI 3170.01E)

**System**: A composite of equipment and skills, and techniques capable of performing or supporting an operational role, or both. A complete system includes all equipment, related facilities, material, software, services, and personnel required for its operation and support to the degree that it can be considered self-sufficient in its intended operational environment. [MIL–STD-721C 6/81]

**Element**: A complete, integrated set of subsystems capable of accomplishing an operational role or function, such as navigation. It is the configuration item delivered by a single contractor.

**Subsystem**: An integrated set of assemblies, components, and parts which performs a cleanly and clearly separated function, involving similar technical skills, or a separate supplier (NCOSE Systems Engineering Handbook V2a [2000]).

**Unit or Subassembly**: A single physical entity containing two or more parts, which is capable of disassembly or part replacement.

**CSCI or SI**: Computer Software Configuration Item/Software Item.

**Part**: A part is a single piece, or two or more joined pieces, which are not normally subject to disassembly with destruction or impairment of the design use. The lowest level of separately identifiable items (e.g., piece parts).

Effective allocation of LYF tests along the integration level will be discussed further in following implementation steps (ref. allocation of LYF tests).

Slide 24

# What about Software?

**The software integration and test process involves four generic stages:**

1. Development Testing
   - *This stage of testing covers Software Unit (SU) testing and integration by the software developers, unit integration testing, and individual Software Item (SI) qualification testing.*
2. Element Testing
   - *This stage of testing includes: integration of multiple Software Items; integration of the Hardware Items (HI) with SIs, and the Element Acceptance Test (EAT) that may also be referred to as the "Factory Acceptance Test" (FAT).*
   - *It normally takes place at the Segment Level depending on where the software entities are developed.*
3. Segment Testing
   - *This stage of testing takes place in a location where elements are integrated and SI/HI elements are tested with other SI/HI elements.*
   - *Includes the functions of Installation, Checkout and Test plus Interface Testing.*
   - *This stage of software testing is normally concluded with a Segment Acceptance Test (SAT).*
4. System Testing
   - *This stage of testing is focused on the process of integrating all of the segments (and sites) into the full system or portions of the full system being tested.*
   - *This stage of testing is normally concluded with a System Qualification Test (SQT)*
   - *Software has a support role in segment and system testing as those activities are typically the responsibility of System Engineering Integration and Test (SEIT).*

24

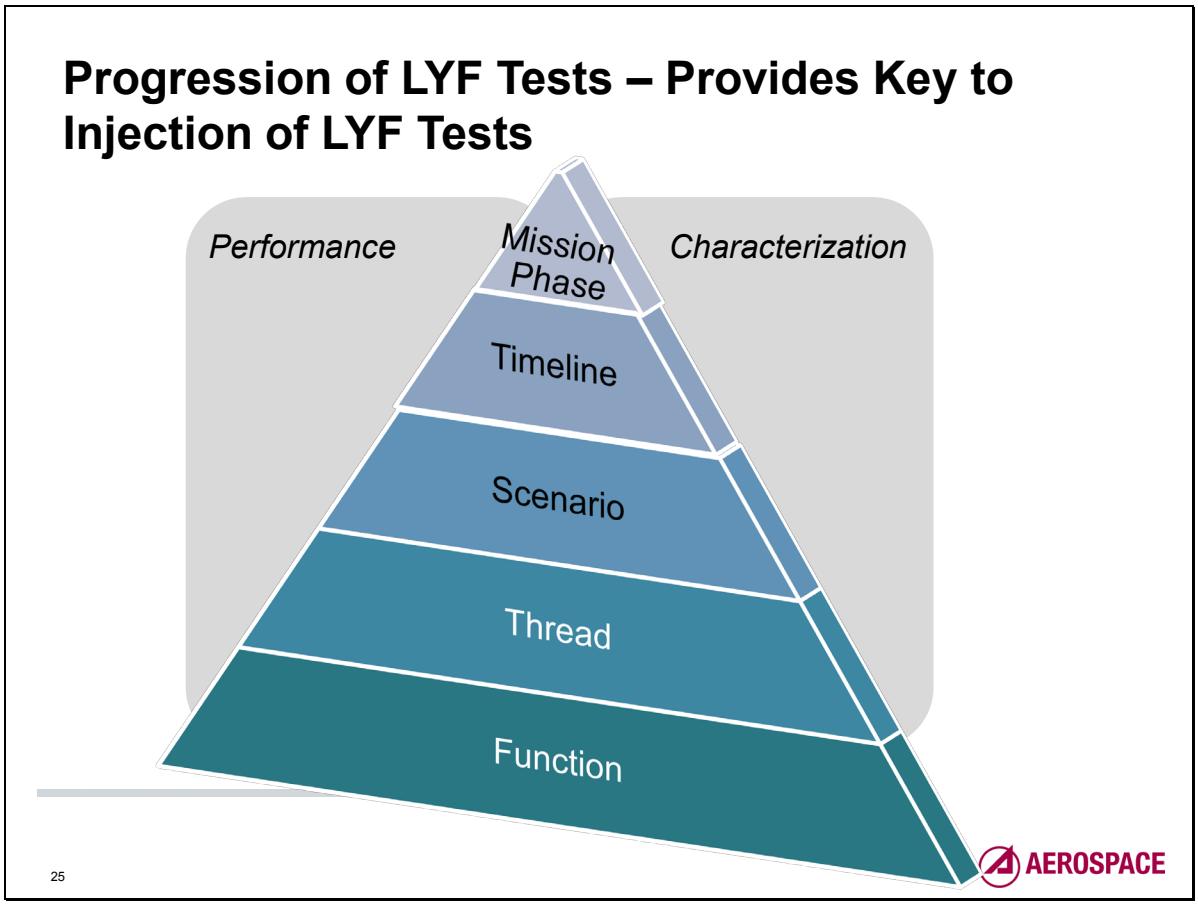
AEROSPACE

Perceptive tests are effective at identifying failure modes and adequately characterizing the item's response to test variables. The test pyramid, shown in the figure, is a generally recommended approach to testing. The philosophy behind this technique is that it is most effective to find failures at the lowest possible level. It is less expensive to test and rework at lower levels of integration. Test perceptiveness is generally higher at the lower levels of assembly. Some types of testing may have better instrumentation or have better access for certain measurements at the lower levels of assembly. There is likely to be higher "transparency" at the lower levels of assembly. It may be easier to see into the workings of the items in an input and response sense.

Some subassemblies, for instance a mirror in a sensor payload, may be characterized at the subassembly level. Unit testing is done to verify workmanship and design attributes, and to perform a higher level of characterization. Subsystem testing is performed to verify interfaces, and possibly measure performance parameters. This may be the best place to characterize performance, especially if payloads are considered to be a subsystem.

This point has a direct parallel in flight software testing. Buettner and Hecht define "white box" (as opposed to black box) testing of software units as taking into account the software's internal structure. Examples include branch and path testing. They further state that, "White box testing is typically conducted at the 'unit' level (i.e., the smallest testable component of software)…..(these tests are) rarely conducted at the higher system integration (i.e., the level of software testing where software is integrated with the system) levels." The underlying assumption made is, again, that the demonstrated character will not change as the software is integrated at higher levels, eventually with the flight hardware. This is a dangerous assumption. [Buettner, D., Hecht, M., *Software Testing in Space Programs*, Crosslink, The Aerospace Corporation, Spring, 2005.]

Slide 25




This shows an increase of mission activity complexity from basic mission functions, through mission threads, mission scenarios, and mission timelines up to a full mission phase.

While the term **function** can be used to describe a high level mission function—an action or activity germane to the mission in the broadest sense (e.g., sensing a rocket launch, routing communication signals between users, commanding a satellite)—we are using it here to mean a very low level of activity reflecting a discrete action/response. This is the building block for higher level combinations of activities.

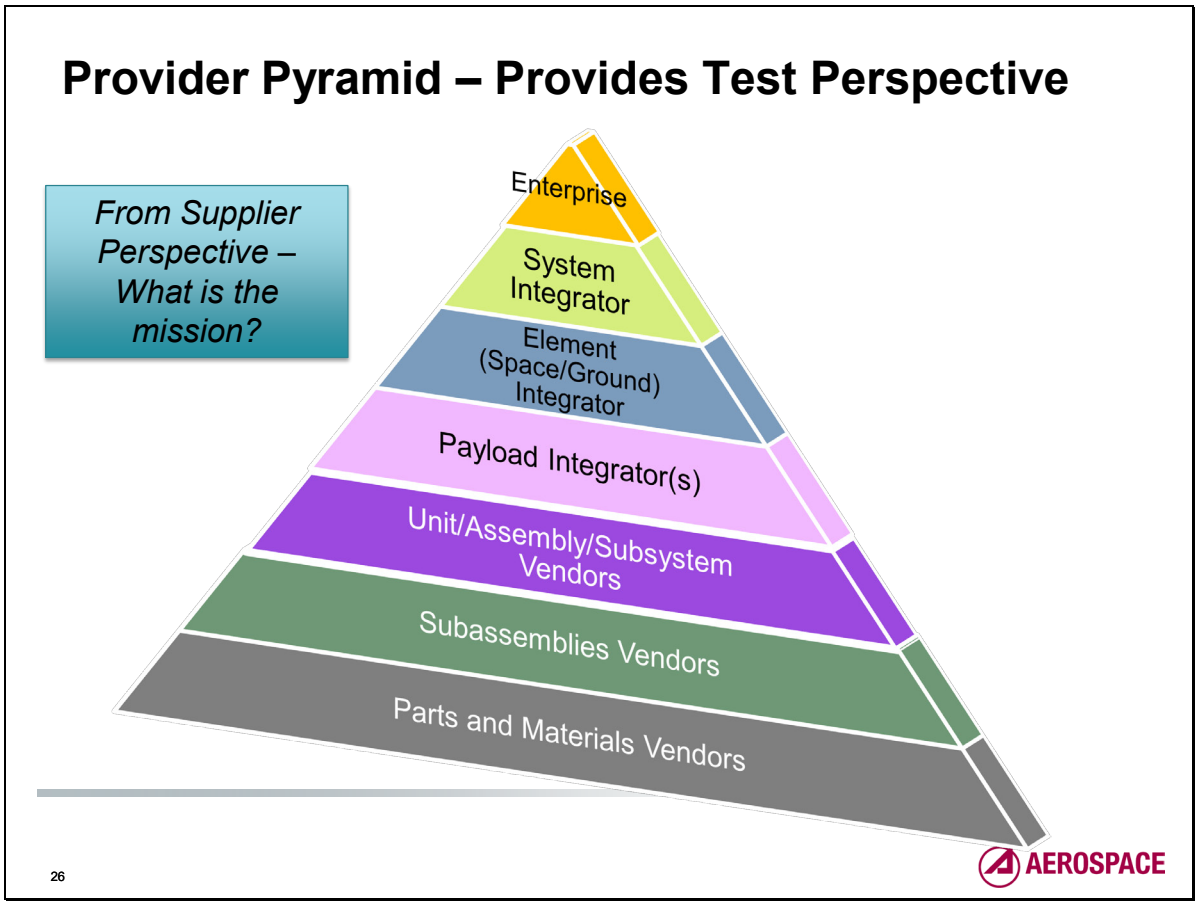
A **thread** is either a stimulus/response pair, or the behavior that results from a sequence of system-level inputs, or an interleaved sequence of system inputs (stimuli) and outputs (responses).

A **scenario** is a brief narrative of expected or anticipated system uses from a user perspective.

A **mission timeline** includes activity order and timing.

A **mission phase** is distinguishable by a discrete change in a key characteristic, such as acceleration, configuration, interaction, or operation.

Slide 26




A recent mission failed because a subassembly designed for continuous operations (100% duty cycle) was delivered to a system that intended to use it at a much lower duty cycle. The provider of subassembly noted that had they been informed of the mission usage, they would have designed something very different. The supplier pyramid provides a representation that should be used to flow applicable mission operations requirements down the supply chain, with an associated validation of that usage in the results from a LYF test. The LYF test at each level demonstrates readiness to perform mission activities at the next higher level of integration. This pyramid culminates in an enterprise level total operations chain/days-in-the-life test as a mission readiness test.

Slide 27

## An Objective of Testing Is to *Find Flaws*

- One of the purposes of testing is to find mission-affecting **flaws** that have escaped detection by quality and other non-test activities
- The purpose of testing is NOT to prove that no **flaws** exist
  - *It is not possible to prove that no flaws exist*
  - *You can only prove that you haven't found any with the tests you have executed*
  - *Systems always have flaws*
  - *Ignorance - anywhere in the system - is also a flaw*
- Finding **flaws** requires multiple levels of robust testing
  - *Thorough, disciplined, and representative of operations*

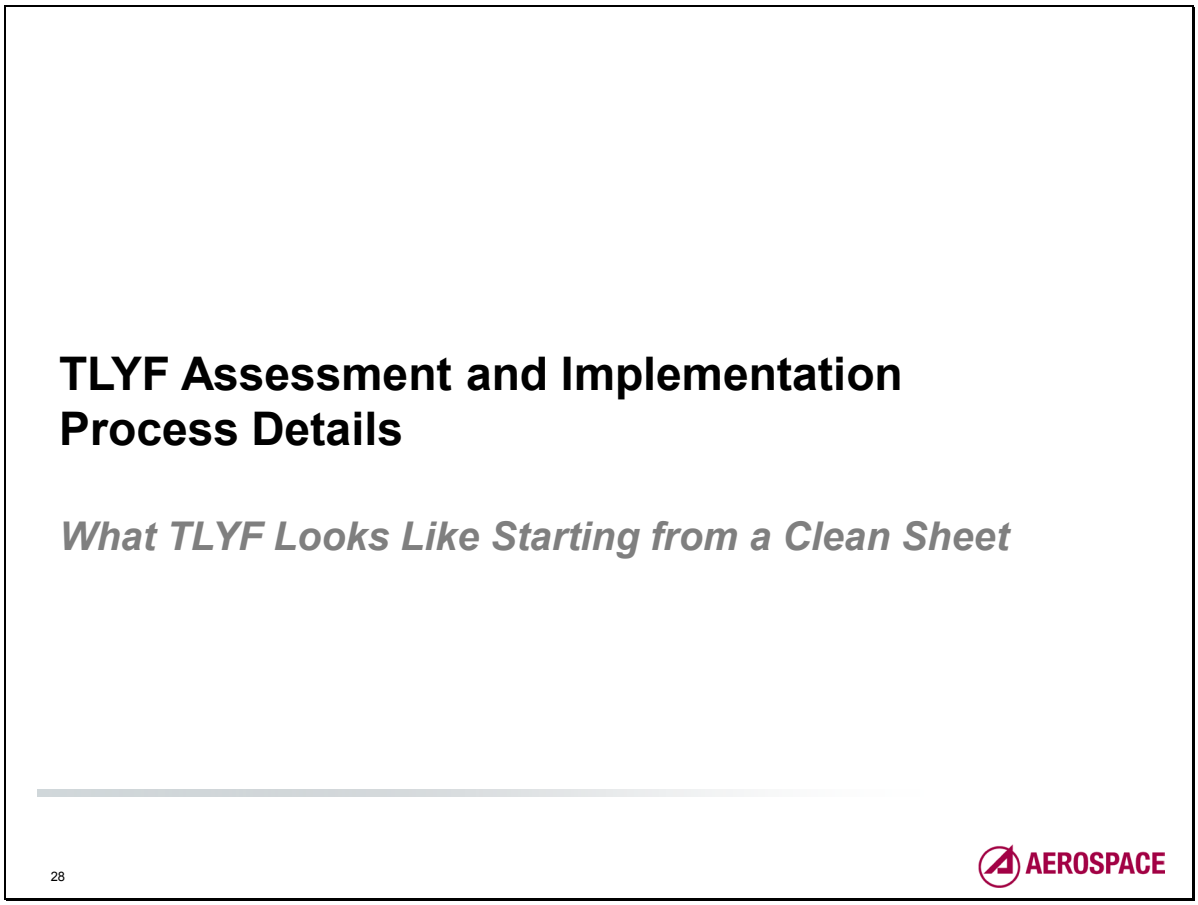
27

AEROSPACE

One purpose of testing is to discover such flaws prior to mission use. When it is not possible to test with all applicable mission characteristics, we must find alternative ways to look for and uncover fatal flaws.

The term "flaw" is synonymous with "defect," "error," "problem," "anomaly," or any other term that can be construed to mean an unintentional behavior of a hardware, software, database, or process that is detectable through an appropriately perceptive test.

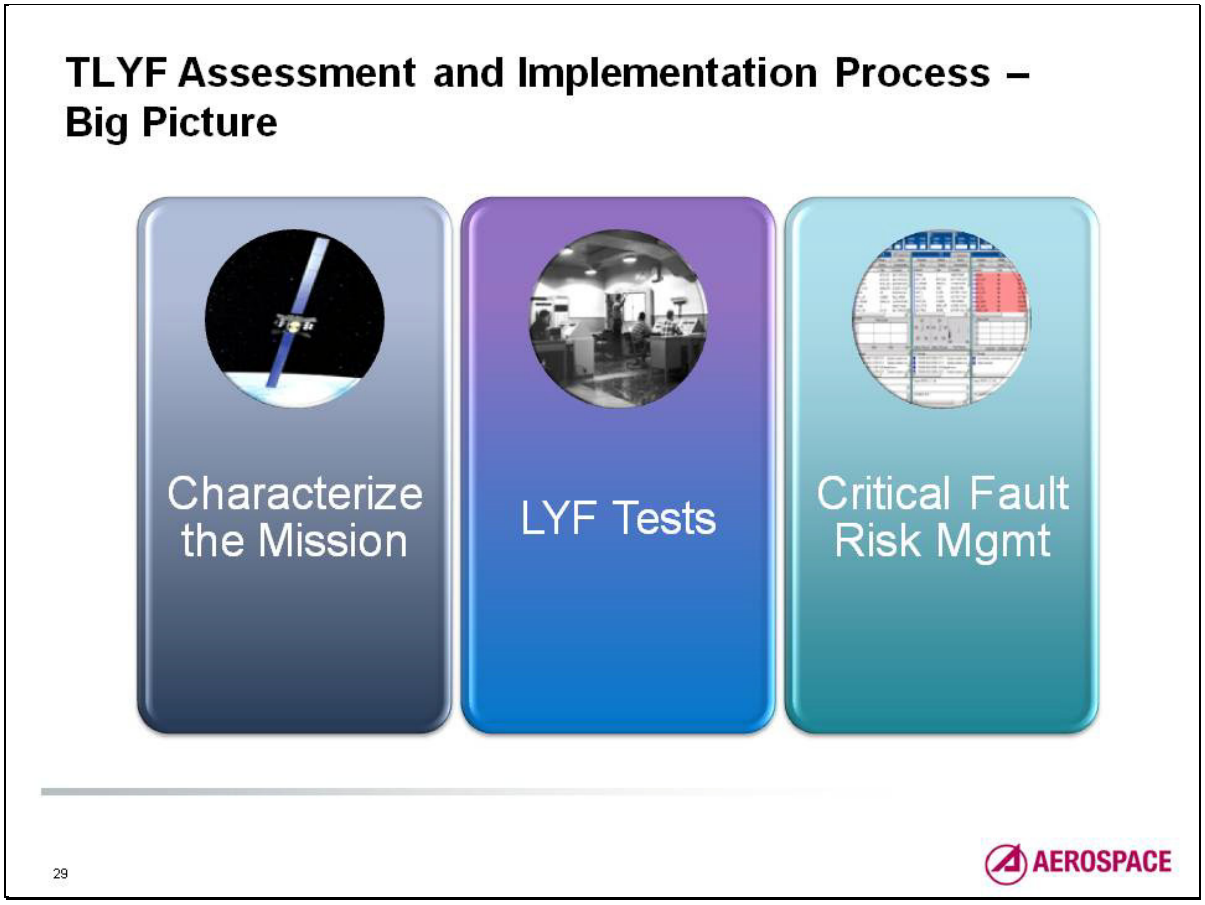
Slide 28




Now, on to the details of the TLYF Assessment and Implementation process.

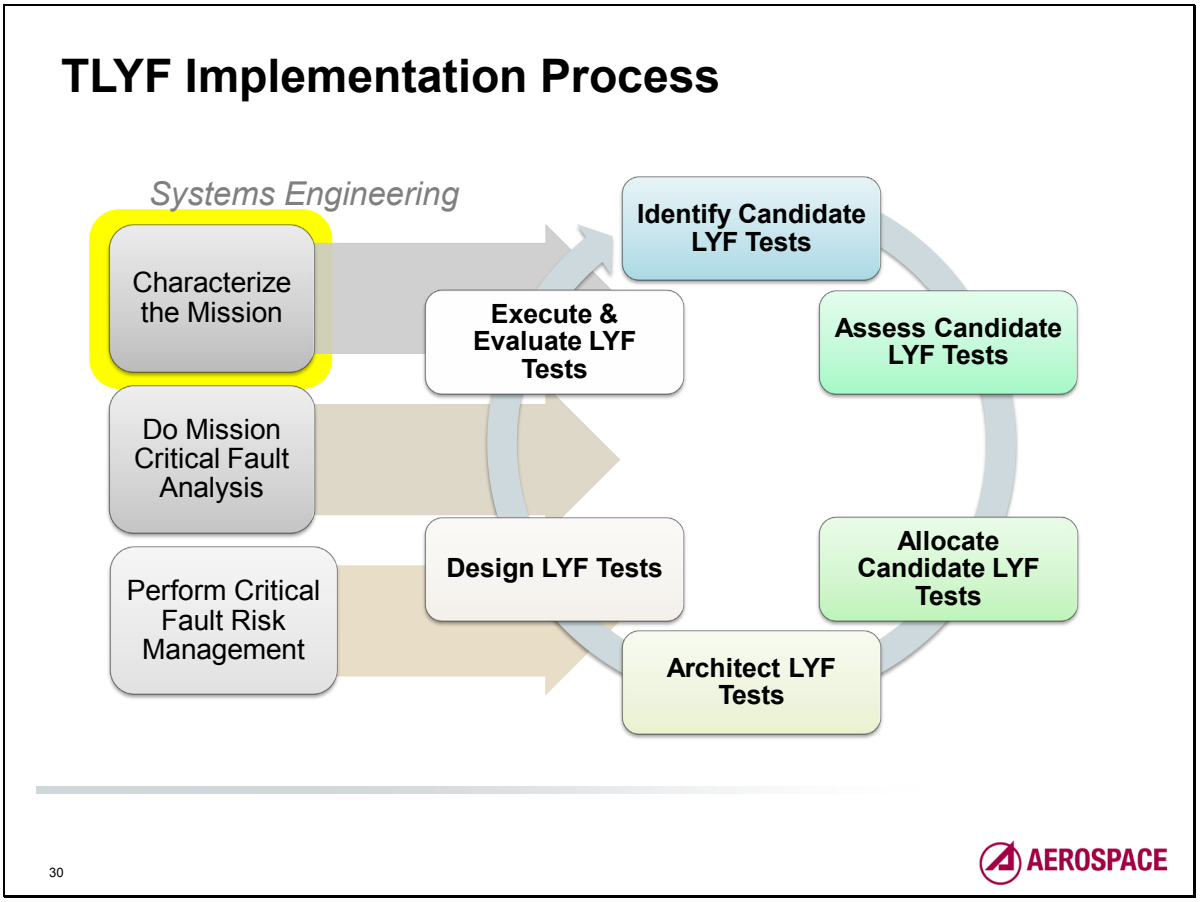
Much of the TLYF implementation process described in this presentation assumes that the approach is applied at the beginning of a program (i.e., Concept Studies Phase). How to apply the TLYF approach while a program is in a later acquisition phase (i.e., at some later point in the development) will be addressed only briefly at the end of this presentation.

Slide 29



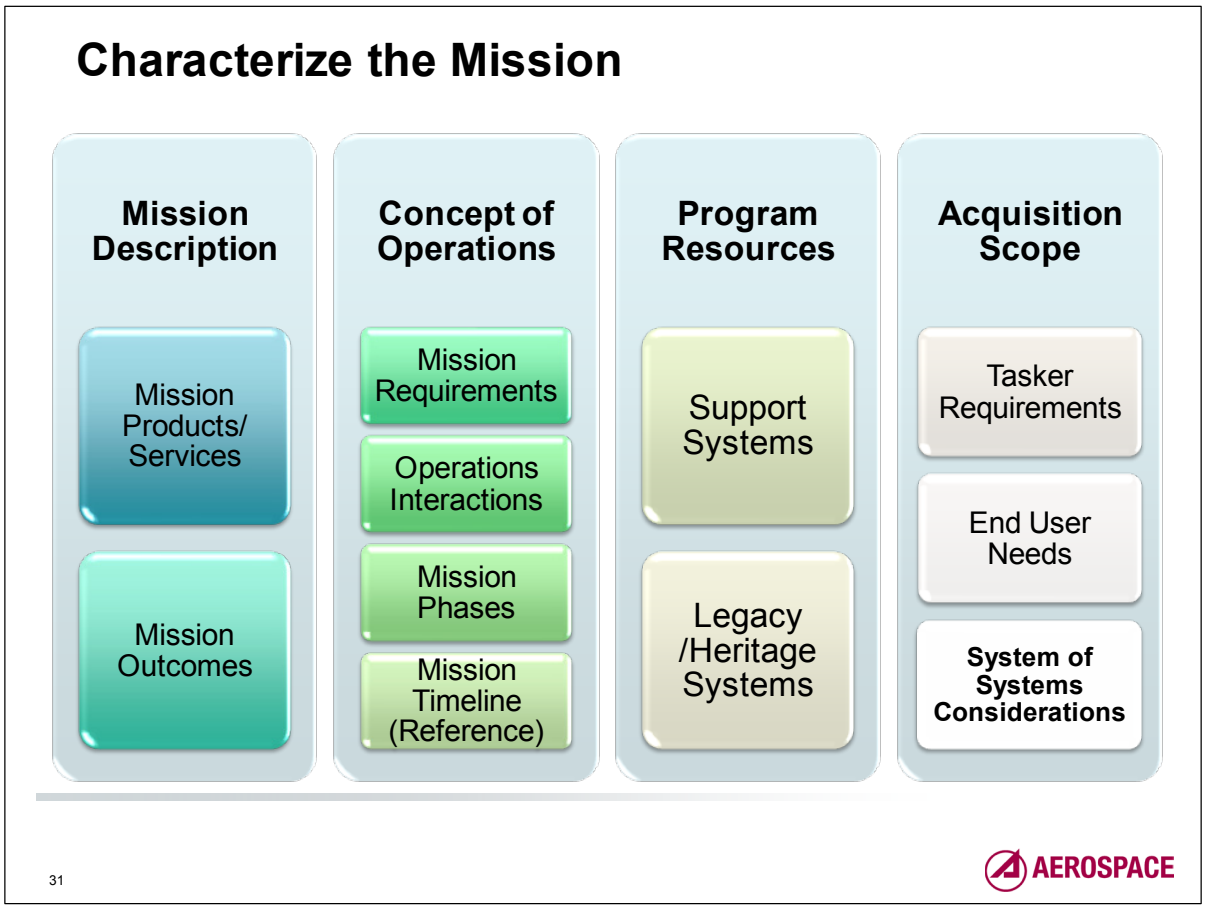

Note: Three parts of the process which will be addressed herein. These make up the major areas of the implementation process: (1) Knowing the mission and all the facets involved in operations, (2) creating, allocating, and conducting the LYF tests, and finally, (3) managing the risks that are highlighted as a result of applying the TLYF process.

Slide 30




The diagram depicts the nine key steps in the TLYF Implementation Process. Each of the boxes will be described in detail, including their inputs and outputs. The process begins with identifying mission operational characteristics. Note the process is circular, conveying the iterative nature of the process. However, the iterative nature of the process does not translate into an endless cycle with no exit. An exit criteria will be laid out at a later point in the presentation. Two of the process steps – Do Mission Critical Fault Analysis and Perform Critical Fault Risk Management – are systems engineering functions that may be chronologically placed elsewhere in the process, but are placed where they are for ease of introducing key concepts for the test aspects of this process.

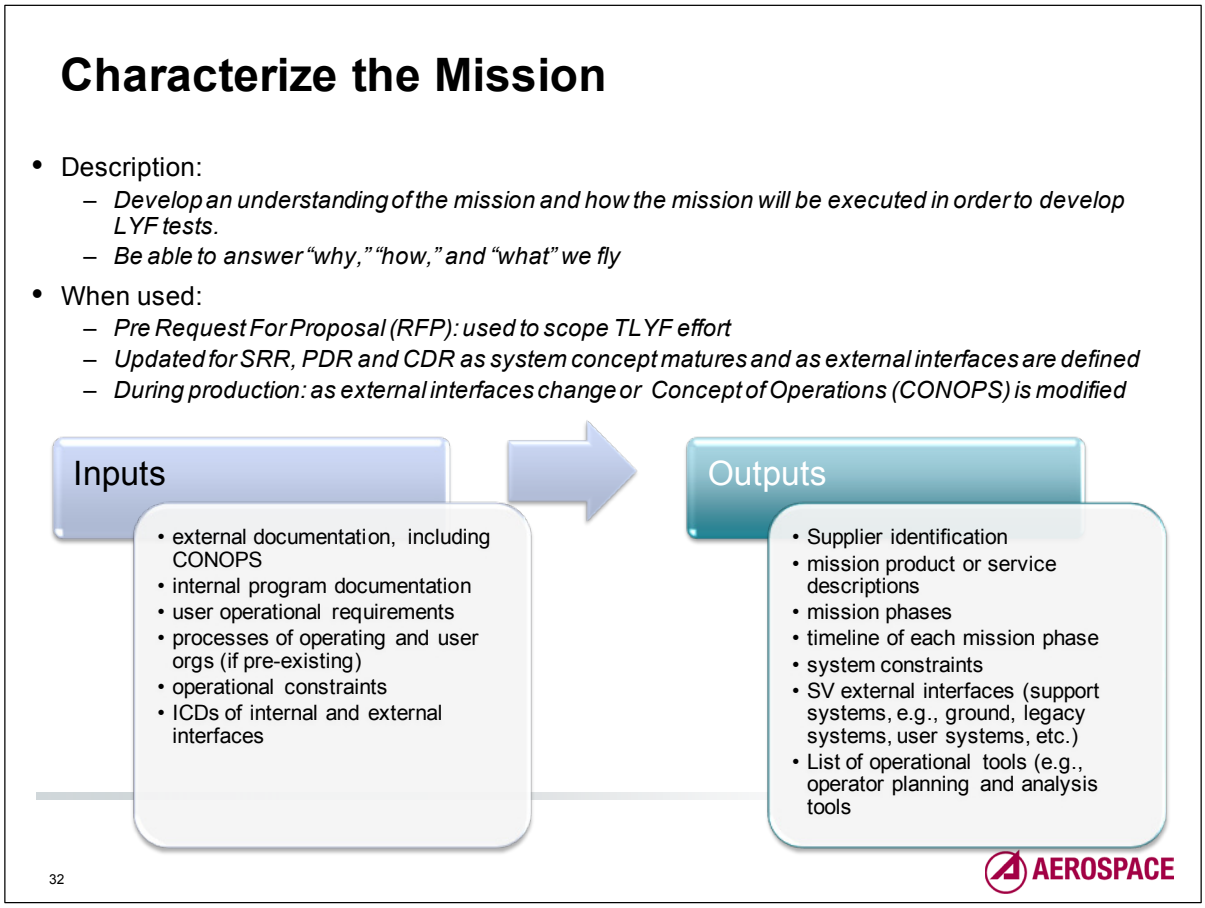
Slide 31




For each step in the process a diagram will be provided which highlights the core aspects of that step. The large shaded boxes are the main pieces and the smaller boxes provide details for those main pieces.

The starting point of identifying the mission requires four basic items: (1) A mission description, (2) the concept of how the system will be operated, (3) a knowledge of the program resources which may interact with the system that is to tested like it flies, and (4) any requirements from the end user need to be obtained because this provides the "purpose" for the system.

Slide 32



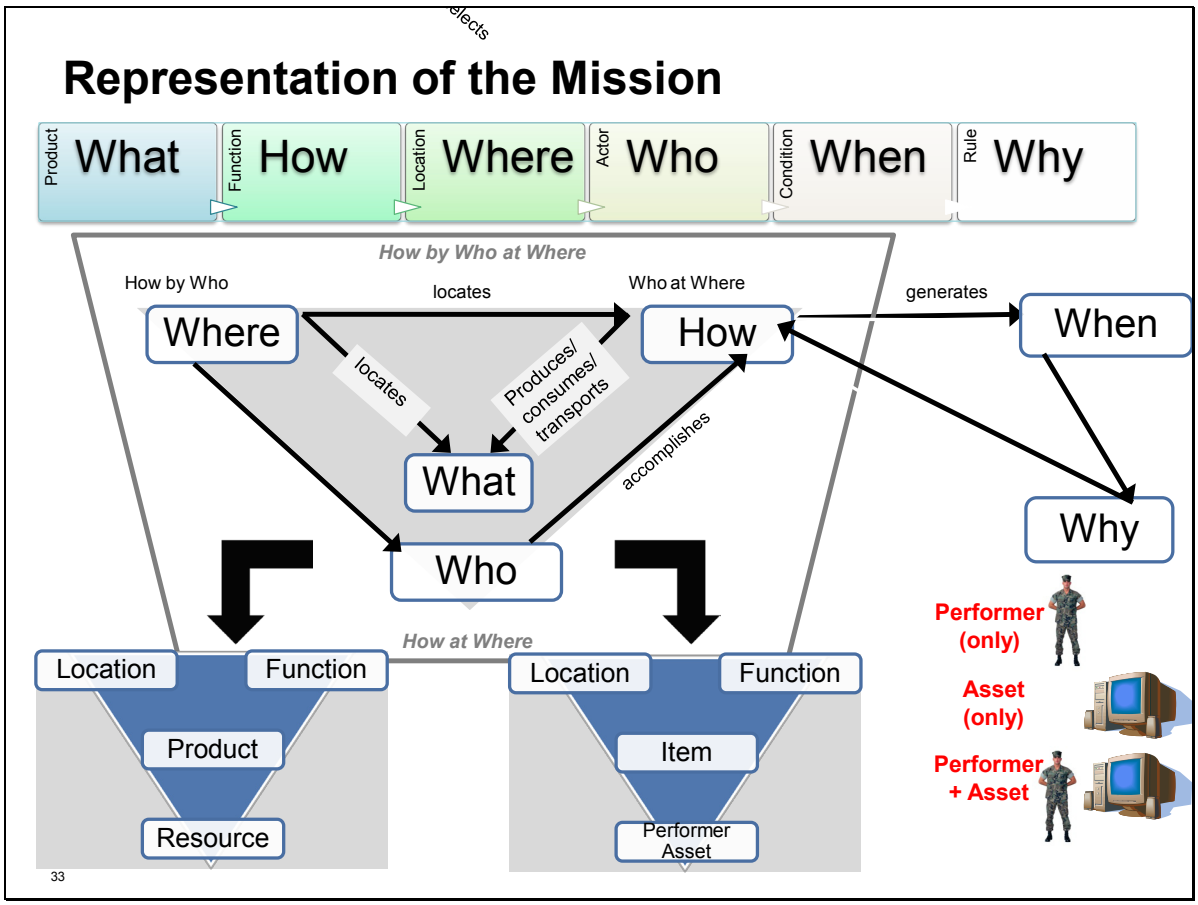

Also, for each step in the process a description of the process will be included along with recommendations for when it can be used during the System Acquisition Lifecycle. The step will also include basic inputs and outputs. Inputs are what is needed to process the step and outputs are items that flow from conducting the step in the process. The maturity of inputs and outputs will depend on several factors, one of which is the status of the system with respect to its lifecycle.

The process begins in the pre-acquisition phase after the initial mission objectives and operations concepts have been baselined. The acquisition team will need to make a series of decisions, that will determine the extent to which the concepts are testable and what items must be acquired or provided to enable those tests.

The parts of the mission concept that are clearly not testable, or are deemed too resource-demanding compared to the value of the project, will form the basis for the initial risk assessment.

| | |
|---|---|
| SRR | System Requirements Review |
| PDR | Preliminary Design Review |
| CDR | Critical Design Review |
| ICD | Interface Control Document |
| SV | Space Vehicle |

Slide 33




The easiest way to make sure you understand the mission is to be able to answer and understand the above questions and their interactions.

The diagram above provides a pictorial representation of a generic mission and helps to draw important questions about the mission. These questions serve as a basis for fostering a TLYF perspective of the system.

Questions raised include, but are not limited to the following:

- Why is the mission being conducted?
- Who is involved in the success of the mission?
- Where are resources located for accomplishing the mission?
- Is there a time constraint as to when data must be transmitted or received?
- What makes the mission successful? It's helpful to think in terms of outcomes. Depending on the type of mission, the answers will vary.
- What are the services?
- What are the products?

Slide 34

## TLYF Basis of Review

- Why We Fly - Mission Objectives
  - *Mission type (products or services)*
  - *Mission contributors (photons in)*
  - *Mission results and products (messages out)*
- How We Fly - Flight Basis
  - *Automated and manual processes*
  - *Space and ground elements*
  - *Mapping flight to test*
  - *Test exceptions to flight and risk of flaw escapes*
- What We Fly - Ready to fly
  - *Flight hardware and software*
  - *Ground command and control hardware, software, processes, tools, and personnel*
  - *Tasking and planning processes, tools, personnel*
  - *For product missions, product creation and distribution processes, tools, and personnel*

34

AEROSPACE

The fundamental basis for the TLYF approach is centered on the notion of flying the mission!

The essence of LYF is a time-driven set of activities that occurs between interacting elements to accomplish mission and support objectives. You must understand how the mission is intended to be executed before you can craft a test or demonstration that emulates flying the mission. Because of this connection between mission operations and test, the TLYF approach has ramifications beyond the confines of a test organization.

TLYF is "joined at the hip" with CONOPS and development, as well as with an understanding of how flaws can interfere with the accomplishment of the mission. Before we can discuss how to test "like you fly" we must first establish how the mission will be flown.

The easiest way to make sure you understand the mission is to be able to answer the following questions: (1) why are we doing the mission? (why we fly), (2) how is the mission accomplished? (how we fly), and (3) what is involved in executing the mission? (what we fly).

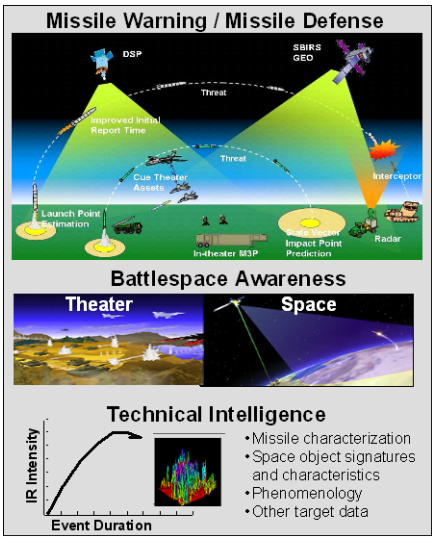
The reason to keep this in mind when discussing TLYF is that the ultimate objective of LYF testing is to ensure that the mission objectives can be accomplished in the context of how and what we fly. There have been many programs whose individual elements met requirements, but failed to accomplish the mission. Subsequent failure investigations have shown that many of these were never tested in the context of achieving mission objectives.

Slide 35

# Why We Fly - Context

- For each type of mission to be successful, a number of events must be successful
- A typical product mission would include something like these events:
  - *Looking at the correct phenomenon in the correct location at the correct time;*
  - *Turning the collected input into raw and/or processed output data;*
  - *Transmitting mission and health data to spacecraft data handling and telemetry subsystems for transmission to a ground station;*
  - *Processing the received data into products and distributing those products to users.*
- A typical communications service mission would include something like these events:
  - *A ground-based satellite transmitter dish beams a signal to the satellite's receiving dish;*
  - *The satellite processes the data and configures according to what is received from the ground*
  - *The satellite boosts the signal and sends it back down to Earth from its transmitter dish to a receiving dish somewhere else on Earth.*

*Space Based Infrared Systems Wing, Col. R Teague, 2 June 2008*




***There have been many programs whose individual elements met requirements, but failed to accomplish the mission.***

35

AEROSPACE

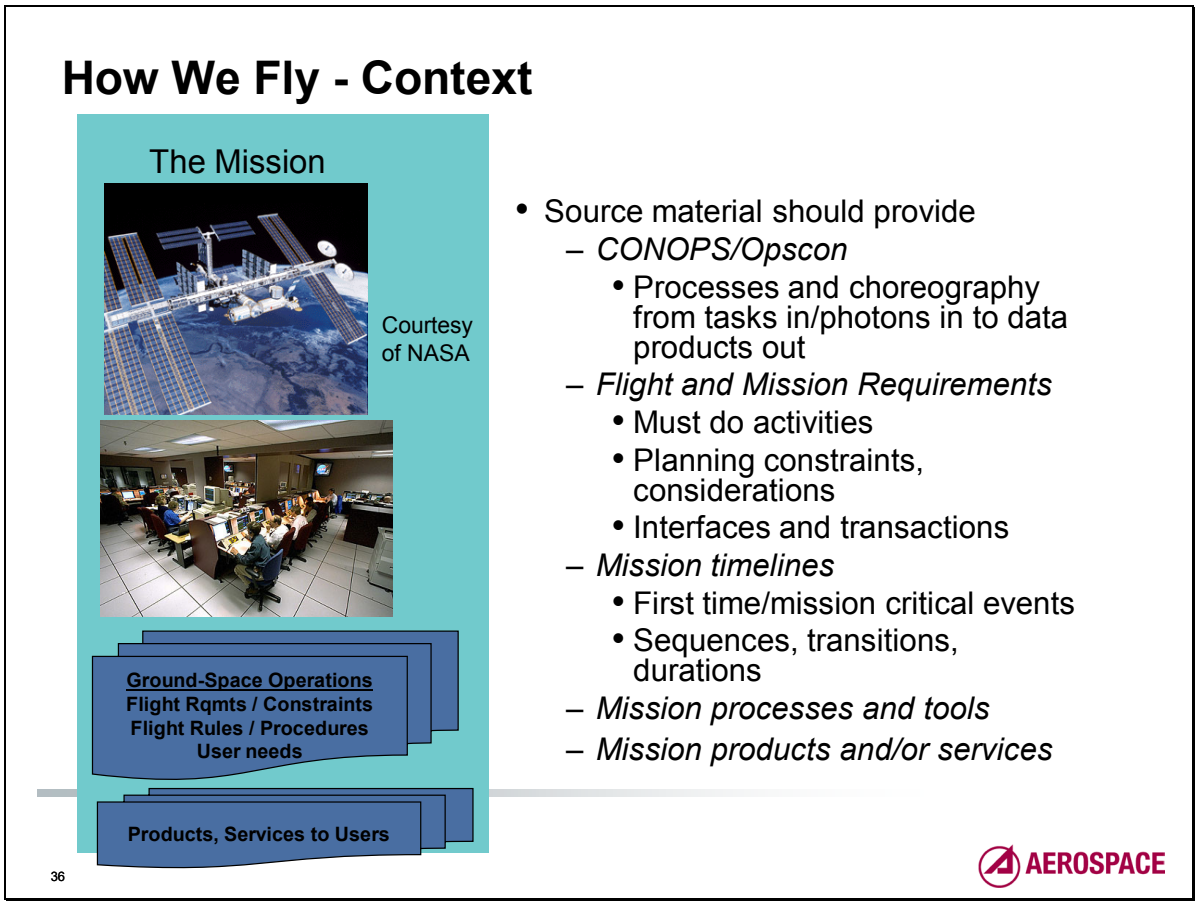
Space missions are generally flown to support government objectives (reference figure above, representing the SBIRS mission).

Most USG unmanned space missions can be put into one of two categories: product missions, and service missions. Product missions use sensors to observe a phenomenon (photons in), return raw and/or processed data to the ground, and perform additional processing of the data on the ground to turn the data in products distributed to users.

There are two primary service missions: communication, and navigation. Communication missions receive owner- or user-generated signals and distribute them to subscriber/other user equipment. The navigation mission provides time and position data directly to user equipment. Most research/development (R&D) projects will also fall into these broad categories.

For each type of mission to be successful, a number of events must be successful. A typical product mission would include something like these events: (1) looking at the correct phenomenon in the correct location at the correct time, (2) turning the collected input into raw and/or processed output data, (3) transmitting mission and health data to spacecraft data handling and telemetry subsystems for transmission to a ground station, (4) processing the received data into products and distributing those products to users. A typical communications service mission would include something like these events: (1) a ground-based satellite transmitter dish beams a signal to the satellite's receiving dish, (2) the satellite processes the data and configures according to what is received from the ground, (3) the satellite boosts the signal and sends it back down to Earth from its transmitter dish to a receiving dish somewhere else on Earth.

Slide 36

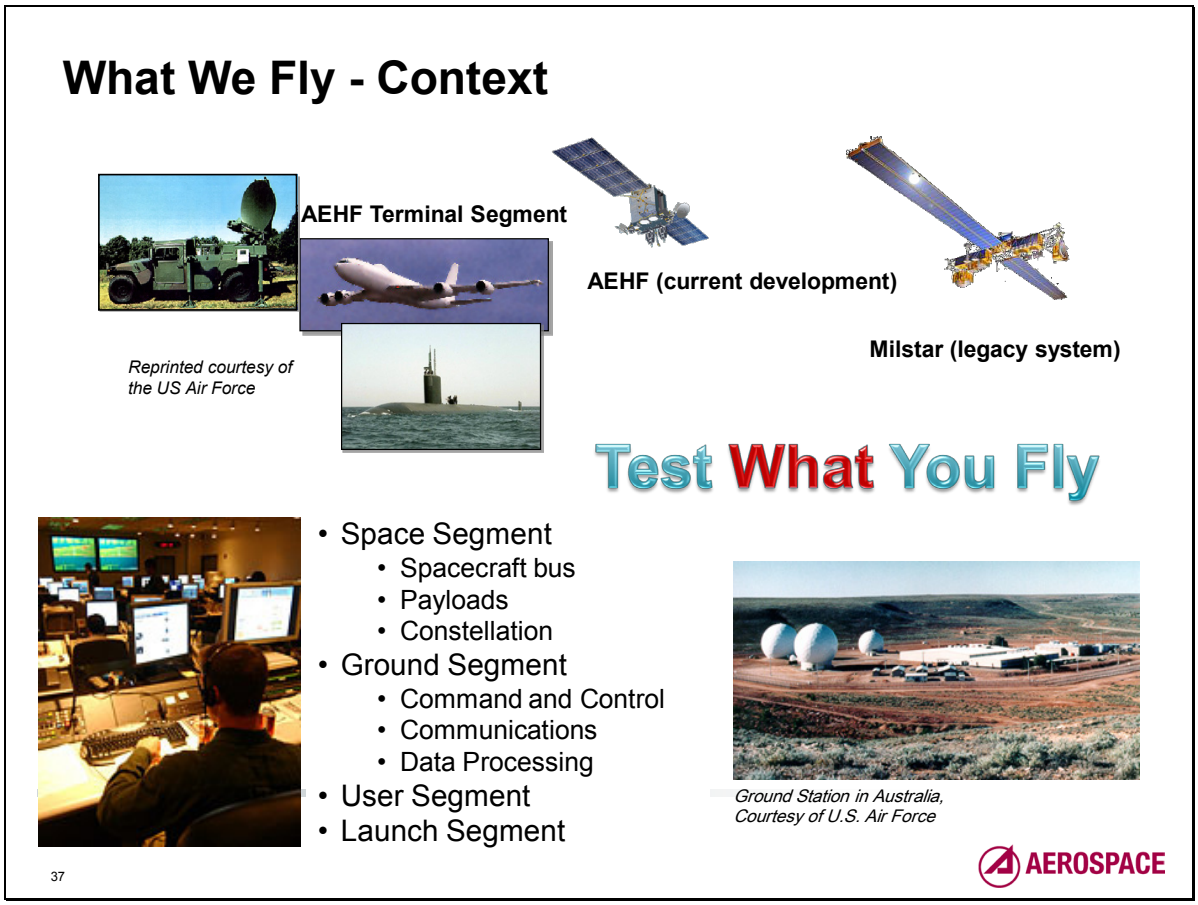



One has to know how the mission is going to be flown before one can define what tests can be done "like you fly." The flight CONOPS is the beginning of a document chain that should explain how the mission will be flown. It is necessary to have early identification of key aspects of mission operations because the manner of use of the spacecraft and payload (P/L) obviously drives the design of both HW and SW.

These aspects include: mission phases, ordering, and priorities; nominal, special, and contingency operations; detailed timelines; time ordered commands and procedures; and mission products and/or services.

Additionally, the CONOPS should include discussions of the people, equipment, SW, and facilities used to fly the mission. Interactions between space and ground control, space and user equipment, tasking agencies to mission planning, ground control to other ground assets, new elements to legacy elements and/or associated systems must all be described. The environments, both physical and operational, through which the mission must be flown need to be defined.

Slide 37



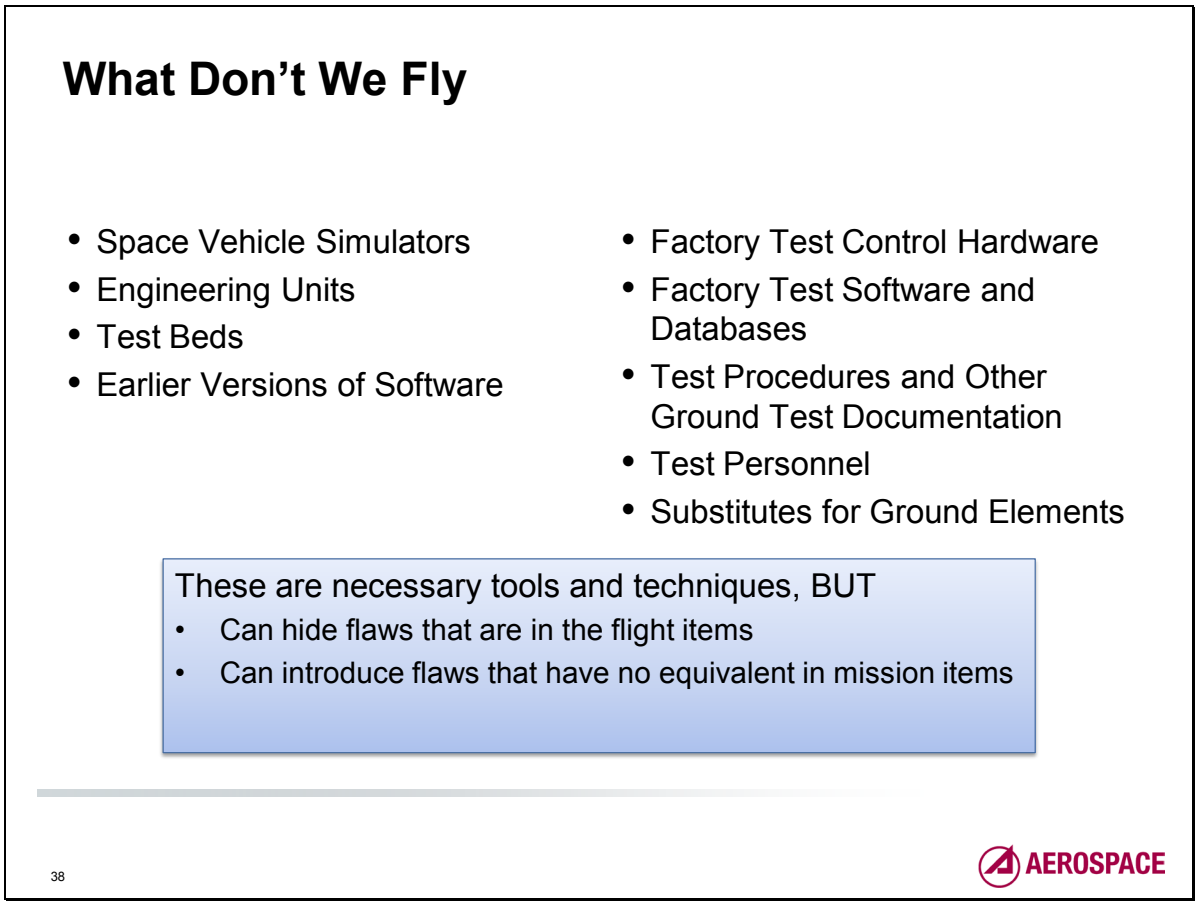

"What we fly" is what must be tested. That would seem to be an obvious notion, but the history of spaceflight is littered with the remnants of failed missions due to a lack of operability tests performed on the actual flight and ground equipment and hardware. Tests done on engineering units and simulators are certainly necessary, but they can't reveal all the flaws that are in the flight system. Tests that reveal flaws lead to repairs. The repaired system is a different entity than the unrepaired version. Tests done on one unit of a series will not reveal flaws on similar, but not identical, units. Tests of the space element that use test equipment for commanding and telemetry are not an adequate substitute for testing the space element with the ground control element. The omission of tests that involve the total operations chain misses the flaws that flow across elements.

TLYF includes the admonition to "Test What You Fly" (TWYF). This means that we must perform tests at appropriate levels of integration of the HW and SW, with the absolute final version of an SV and the ground elements prior to launch with the operational HW, SW, databases, processes, and procedures.

SV HW and SW undergo changes throughout the development and test phases of a program. The decision whether and how to retest is based on a number of factors, including the extent of the most recent change, schedule pressures, and the kinds of tests remaining. The decision should also be based on TLYF aspects, especially for tests late in the vehicle flow (after thermal-vacuum). Studies conducted by The Aerospace Corporation have shown that the risk of a flight anomaly in a unit, with significant rework, replaced late in the integration and test flow, is triple that under normal circumstances. Even apparently minor changes can have profound effects on a mission, especially if those changes are performed incorrectly or damage previously functioning HW. Late repairs tend to

have less rigorous review and control of procedures. Ad hoc repairs are a frequent source of additional problems. Inadequate or no post-rework test of the repaired item is considered a TWYF violation.

Slide 38




Alternatives include, but are not limited to, using non-flight hardware, doing a LYF test at a lower level of assembly, or doing a simulation. All deviations from "what" or "how" you fly should be assessed for criticality and treated as a TLYF exception.

Along with knowing the how, what, and why of flying is the conscious awareness of what is used in testing that is NOT flown. These are necessary tools and techniques, BUT their use hides flaws that only come from the flight items. These items are not cost neutral, even if provided by contractor. Their use introduces flaws that have no relation to mission items.

*Form, fit, and function is not TLYF.*

Examples include the following:

- Space Vehicle Simulators
- Engineering Units
- Test Beds
- Factory Test Control Hardware
- Factory Test Software and Databases
- Test Procedures and Other Ground Test Documentation
- Test Personnel

Slide 39

## Possible Mission Phases

| Mission Phase | Definition |
|---|---|
| Ascent | T+0 through LV Separation |
| Automated Initialization | SV initialization activities under the control of pre-loaded command list |
| Orbit Transfer | From first orbit determination until SV is in operational orbit. (May overlap SV commissioning) |
| SV Commissioning | From the time automated initialization completes until the SV is ready to operate. |
| Normal Ops | Ready for ops through special ops or End of Life (EOL) |
| Fault and Contingency | Begin when conditions force the SV from normal operations ; end when the SV returns to normal operations. |

39

AEROSPACE

Each mission can be thought of in discrete operational phases. Each phase needs to be considered when exploring candidate LYF tests. The chart lists possible mission phases. A mission phase should encompass all the activities that occur during the phase. Thus, if orbit transfer activities and SV commissioning activities occur simultaneously, the mission phase should encompass both. For a candidate LYF test, it is important that all the activities that occur within a given phase be considered on the timeline so that operationally representative interactions occur. It is also necessary to consider candidate LYF tests that cross mission phase boundaries and that account for possible variations in phase transition entry and exit conditions.

We are including Fault and Contingency operations as a distinct phase. Note that while the other phases have a single expected timeline, the Fault and Contingency phase will have a timeline and set of activities based upon the particular anomaly that occurs. Faults and contingencies that are applicable in each of the regular mission phases will need separate candidate LYF tests for each phase.

Slide 40

## Mission Characteristic Classes

- The primary attribute about the way we conduct a mission is the concurrency of characteristics
- Characteristic classes include:
  - *Time and Timeline*
  - *End-to-end (integration) level*
  - *Configuration*
  - *Environments (Internal, Ascent, Space)*
  - *Commands*
  - *Telemetry (State of Health, mission data)*
  - *Mission Planning and Operations*

***There's More to Flight than Configuration and Environments***

40

AEROSPACE

Mission activities are the normal, intentionally executed functions that prepare and carry out the mission. Examples of mission activities include: booster stage separation, collision avoidance, space vehicle contact with ground station, entrance into umbra, solar array deployment, acquire and track a target, uplink a command load, and broadcast a timing signal. Mission events are noteworthy happenings, whether planned or unplanned. Examples include: first light through an optical system, loss of signal (unplanned), transition to safe mode, or transition to operational status.

Mission characteristics are aspects specific to the mission objectives including mission: phases and modes, tasking, mission and command planning, timelines, event sequences, operational constraints, operational considerations, signal services, and data products. Mission characteristics can be grouped into "characteristic classes." Each class has a number of associated characteristics. For example, the LYF characteristics of the Time and Timeline class include, but are not limited to: continuous clock, timing, duration, order/sequence of events, and duty cycle. The Time and Timeline characteristic class is the primary aspect of a LYF test.

For each test that must be "Like You Fly," determine which mission characteristics must be included as part of the test. A LYF test must be cognizant of an appropriate set of initial conditions for the mission phase. A LYF test includes a set of time-ordered events that include transactions and interactions among the elements included in the test.

LYF tests at each level of assembly should have as many applicable mission characteristics included as possible. Lower level tests of first time- and mission-critical activities should be designed to focus on the most germane characteristics to the activity. Where it is not possible to include certain key

characteristics, or characteristic combinations, a TLYF exception should be noted. TLYF exceptions need to be evaluated for criticality, as discussed in the Step 5: Do Mission Critical Analysis, and possibly included in Step 9: Perform Critical Fault Risk Management.

Tests that are not primarily intended as LYF tests by this definition will need applicable mission characteristics included as appropriate with regard to requirements and test objectives.

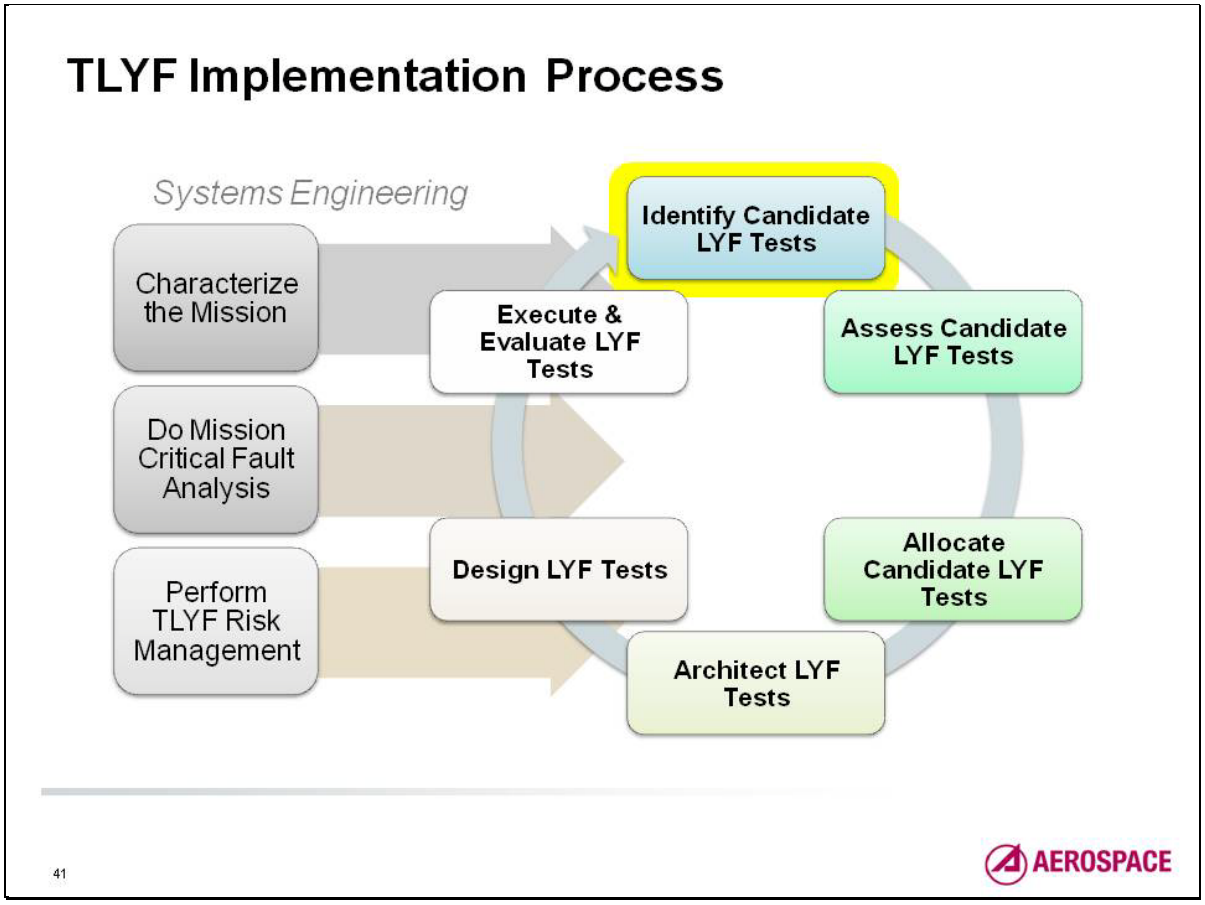
| | | |
|---|---|---|
| **End-to-end Level** | **Time and Timeline** | **Ascent Environments** |
| Component | Clock Reset | Random Vibration |
| Unit | Test driven function order | Sine Vibration |
| Subsystem | Test initial conditions | Acoustic |
| Flight Software (Bus) | Test Duration | Shock |
| Payload Software | Test recurrence rate | Ambient Pressure |
| Payload | Running Clock | Ambient (Room) Temperature |
| Space Vehicle (SV) | Pre-programmed/Invariant command sequence | Conducted/Radiated EMI/EMC |
| Space Segment | Fixed Duration Activity | Vibroacoustics |
| Launch Vehicle | Variable Duration Activity | Shock Events |
| Ground Element | Order Dependent Activity | Acceleration |
| Ground Segment | Order Independent Activity | Booster RF |
| System (SV + Ground Control) | Initial Conditions | Near Space RF |
| End-to-End SYSTEM (Space segment + ground segment) | First Time Activity | Ascent Temperature Profile |
| System of Systems | Occasional Recurrence | Ascent Pressure Profile |
| **Configuration** | Regular Recurrence | **Space Environments** |
| Test Article | Mission Phase Specific | Ramps to Hot & Cold Temperature Plateaus |
| Test Equipment | Mission Phase Independent | Vacuum |
| Test SW | Contact (Communication) Constraints | Atomic Oxygen |
| Facility | **SV Internal Environments** | Eclipse Duration |
| Simulator | Sine Vibration | Eclipse Transitions |
| Support Functions | Acoustic | Sun Duration & Angle |
| SV (with config exceptions) | Shock | Solar Radiation |
| Space Assets | Conducted/Radiated EMI/EMC | Planet Albedo |
| Ground SV Control (Uplink) | Vibroacoustics | Man-Made Earth-Origin Optical |
| Ground PL Control (Uplink) | Shock Events | Man-Made Earth-Origin RF/Radar |
| Command Database | SV RF EMI/EMC | Atmospheric Layer Emissions |
| Telemetry Database | Temperature Variations | Auroral Emissions |
| Downlink Assets | Inertia | SAA |
| Mission Tasking | **Services** | Cosmic & Belt Particles & Waves |
| Mission Planning | *Collective operations* | Gravity |
| User Equipment | *Content-based and Policy-based Routing* | |
| Data Production | *Communication scop* | |
| Data Distribution | | |

| **Commands** | **Mission Data** | **Mission Planning & CONOPS** |
|---|---|---|
| Command Hard line | Bands/Rates | Mode Dependent |
| Test command script | (Near) realtime Evaluation | Mode Independent |
| Test command database | Integration of SC + PL Data | Automated Fault Management |
| Bands/Rates | Data Production Tools | Payload Planning |
| Contact Command Plans | Data Production Personnel | Mission Personnel |
| Time-tagged Commanding (CMD Uploads) | Data Production Transactions | Mission Procedures |
| Real-time Commanding | Data Distribution Tools | Mission Processes |
| Command Options | Data Distribution Transactions | Mission Phases |
| **SOH TLM** | Data Archive Tools | Mission Planning |
| Telemetry Hardline | Data Archive | Inter-System Transactions |
| STE limit checking | Data Retrieval Tools | Intra-System Transactions |
| Test TLM database | Data Retrieval | Interagency Transactions |
| Bands/Rates | | |
| Automated (ground) limit telemetry checking | | |
| Stored Telemetry Playback | | |
| Manual, Realtime TLM Evaluation | | |
| TLM Trending & Evaluation (Tools) | | |
| TLM Evaluation (Personnel) | | |

[1]

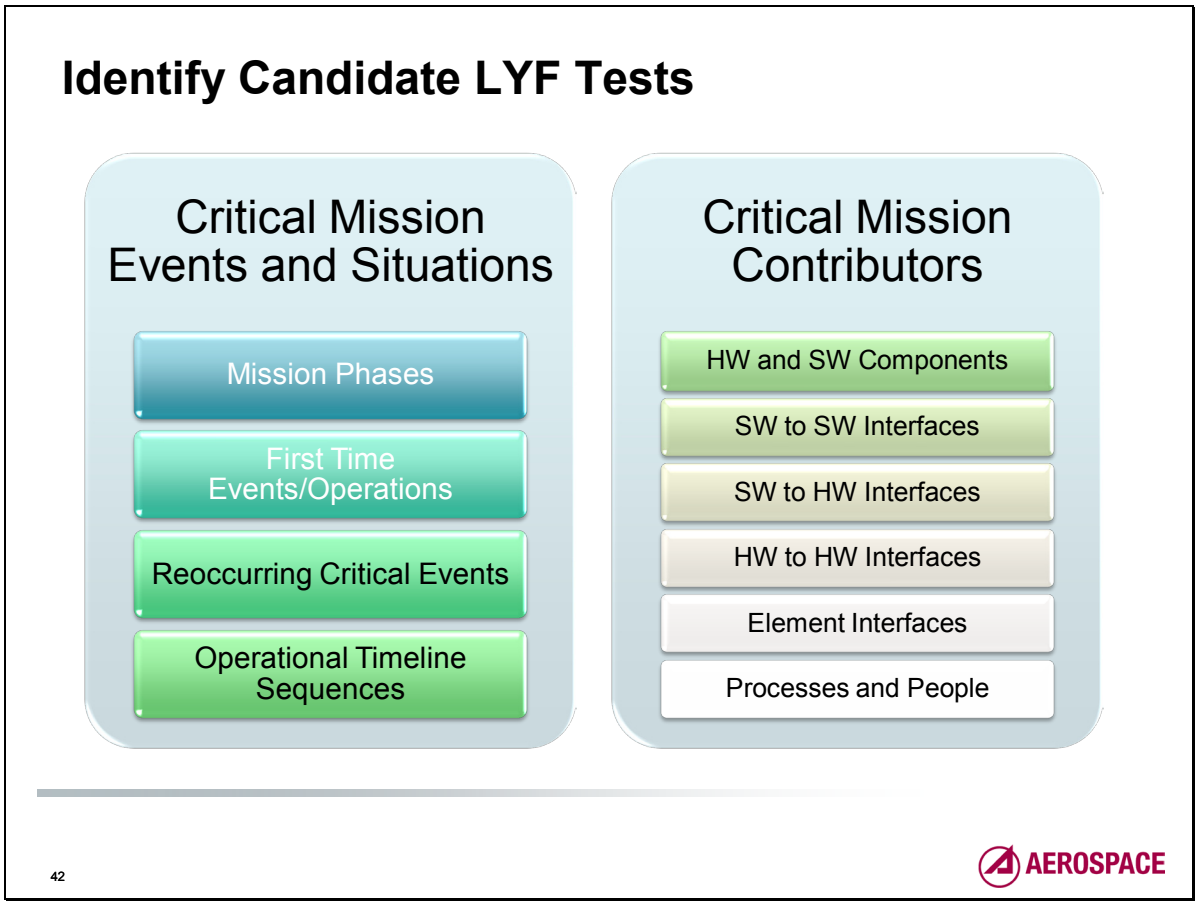
[1] Note: items in black are flight/mission characteristics; items in other colors are test related approximations/alternatives to flight/mission characteristics

Slide 41




The next three steps of the process, Identify, Assess, and Allocate Candidate LYF Tests are closely coupled and result in the definition of the LYF tests for the program. In practice, when identifying a candidate test, the engineer may immediately assess and allocate it. However, the steps have been separated for this discussion in order to highlight the salient features of each step.

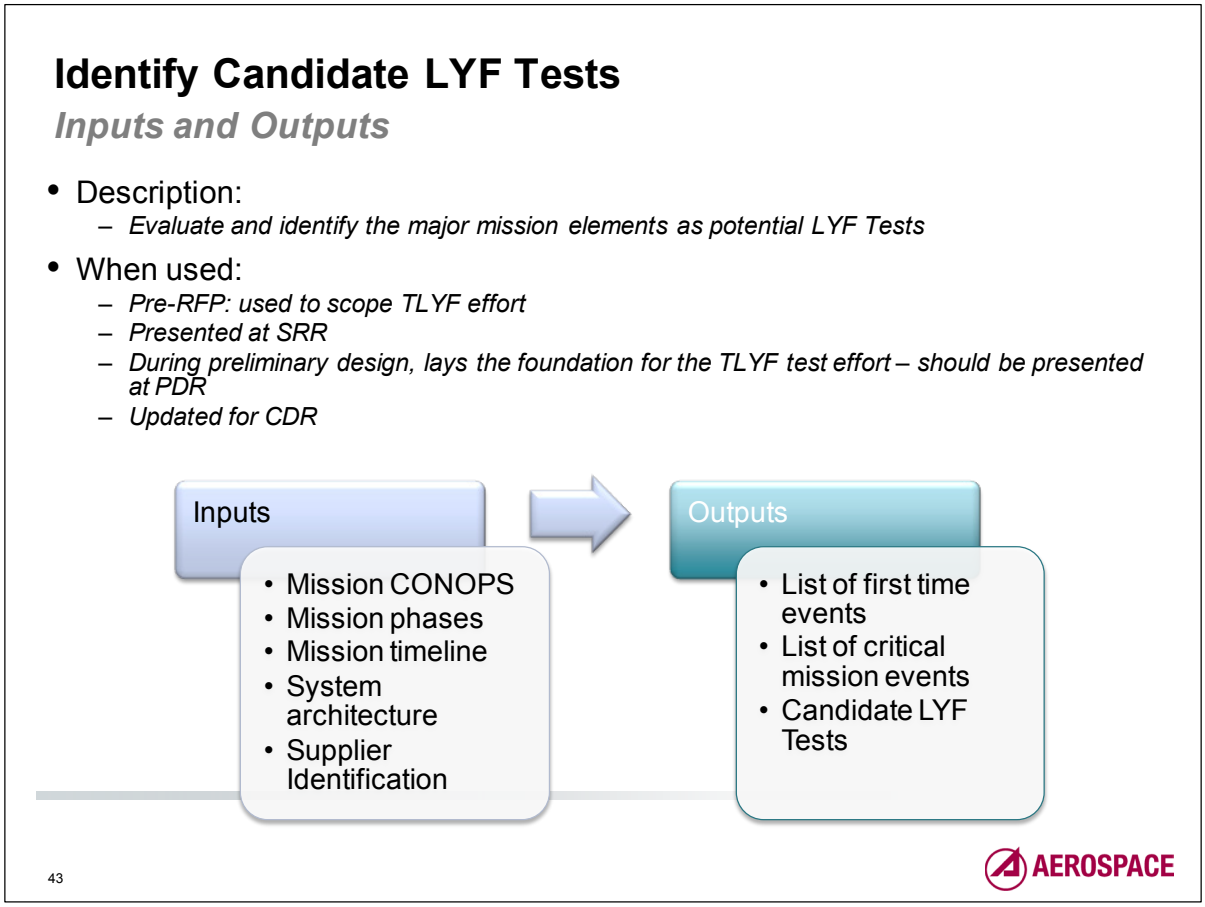
Slide 42




In identifying candidate LYF tests, the system engineer evaluates the mission and selects those mission situations that should be subject to LYF tests. This is done by looking across at the mission, across all mission phases – including the fault and contingency phase – to identify first time events and operations, recurring critical events, and operational sequences. For each of these potential situations, the critical mission contributors to the situation are identified, to provide an initial scope for the LYF tests.

Note that the succeeding steps will address the feasibility of performing the LYF test at the highest integration and function levels and the allocation of tests to both the highest feasible level and to lower levels of the integration and function pyramids as necessary for practicality and risk reduction.

Slide 43



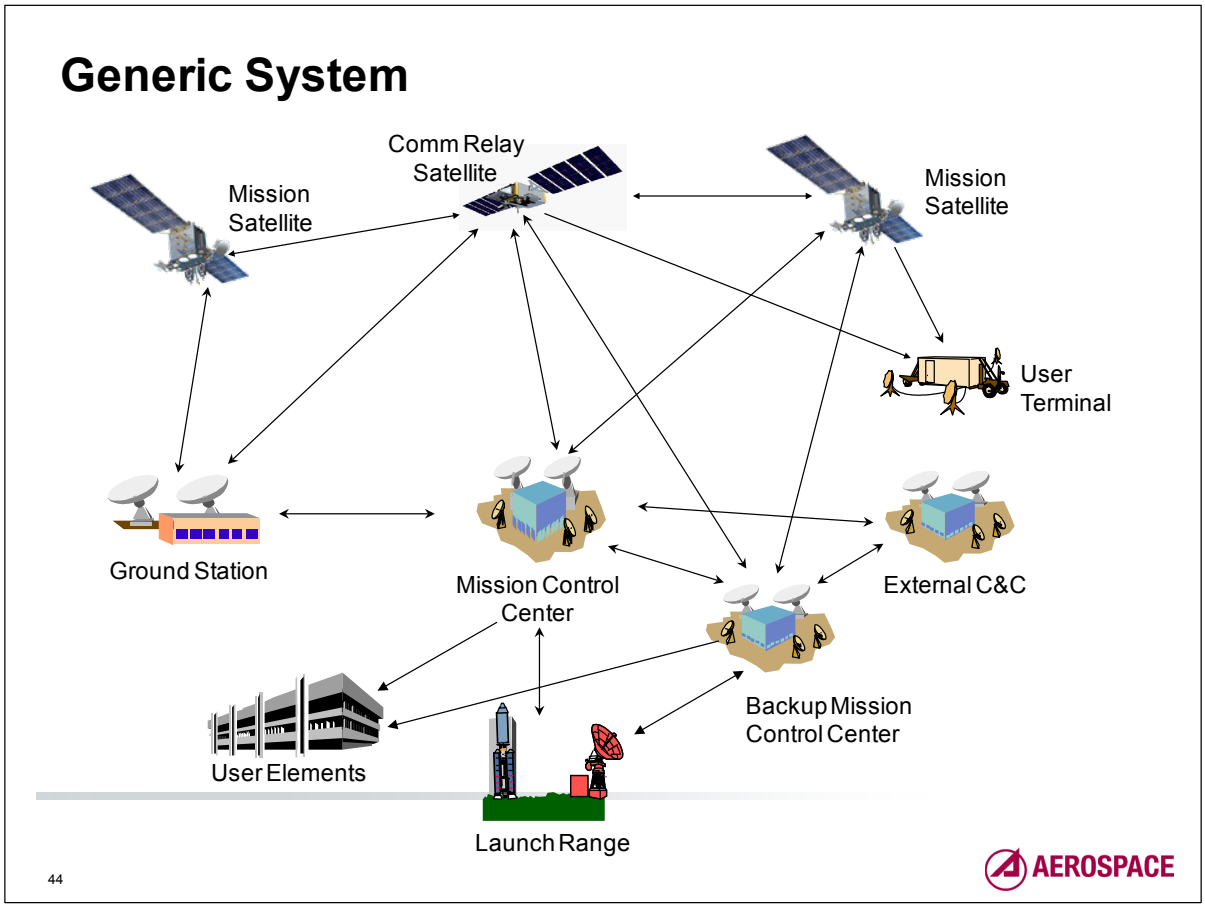

This step, as well as the next two, is first done at a high level by the **program office** in order to estimate the effort (cost and time) involved and to identify any special resources that will be needed for the TLYF validation. For instance, if the vehicle under development has an optical instrument, the total TOCT needed to validate mission performance might require a scene simulator in the TVAC chamber as well as communication connections between the vehicle in the TVAC chamber and the operational ground system. The program would want to include those costs in the initial estimates and might need to include a TLYF requirement in the RFP.

The test "item" and operational timeline to be used for the test should be clearly defined, with the candidate tests defined at the highest relevant level of the integration and function pyramids. For instance, in the case of a LYF test of the normal operations of an optical sensor, the test "item" might include not only the SV and ground command system, but also mission data processing and mission tasking. The operational timeline would include all the activities that would occur during a continuous, several-days period of operations. These activities might include: routine space vehicle activities (e.g., command schedule uploads, state of health checks, stored state of health downloads); mission operations based on long-term tasking (e.g., long-term schedule uploads, mission data downloads, mission data processing and dissemination); and interleaved periods of high-priority, quick response tasking (e.g., upload of new tasking files or direct tasking commands, selective high-priority downloads, and special data processing).

Successful completion of this step includes two lists gleaned from all available mission information, including various supplier perspectives: (1) first time events and (2) mission critical events. These lists will help provide the basis for initial Candidate LYF test list.

As the design and the CONOPS are refined, the candidate tests will become more specific.

Slide 44




This notional chart shows some of the various elements that might be included in a system. A LYF test at the system level of the integration pyramid must consider all relevant elements, for the specific system, in defining the candidate LYF tests.

For instance, if the satellite initialization phase will be run autonomously on-orbit, a LYF test of this sequence would not need to involve the ground segment. However, a LYF recovery from an anomalous initialization sequence (fault and contingency phase operation) would involve the SV, ground segment, operations personnel, and operational procedures. A LYF normal operations test would also involve user elements.

| | |
|---|---|
| Space Segment | Mission satellites, COMM Relay Satellites |
| Ground Segment | Ground Stations, Mission Control Center (MCC), External C&C Center |
| User Segment | User Terminal, User Elements (e.g., data processing center) |
| Launch Segment | Launch Range and related facilities |
| C&C | Command and Control |

Slide 45

## Some Candidate LYF Tests

- Total Operations Chain/Days or Weeks in the Life
- A really bad day in the life
  - *Stressing mission operations*
- Ascent Phase
- Orbit Transfer
- Automated initialization
- Defined fault situations (Programmed/Planned)
  - *Automated fault management*
  - *Redundancy management*
  - *Entry into safe mode*
  - *Error detection and correction*
  - *Operational planned response contingencies*
- Planned contingencies
  - *Recovery / exit from safe mode*
  - *Program specific*

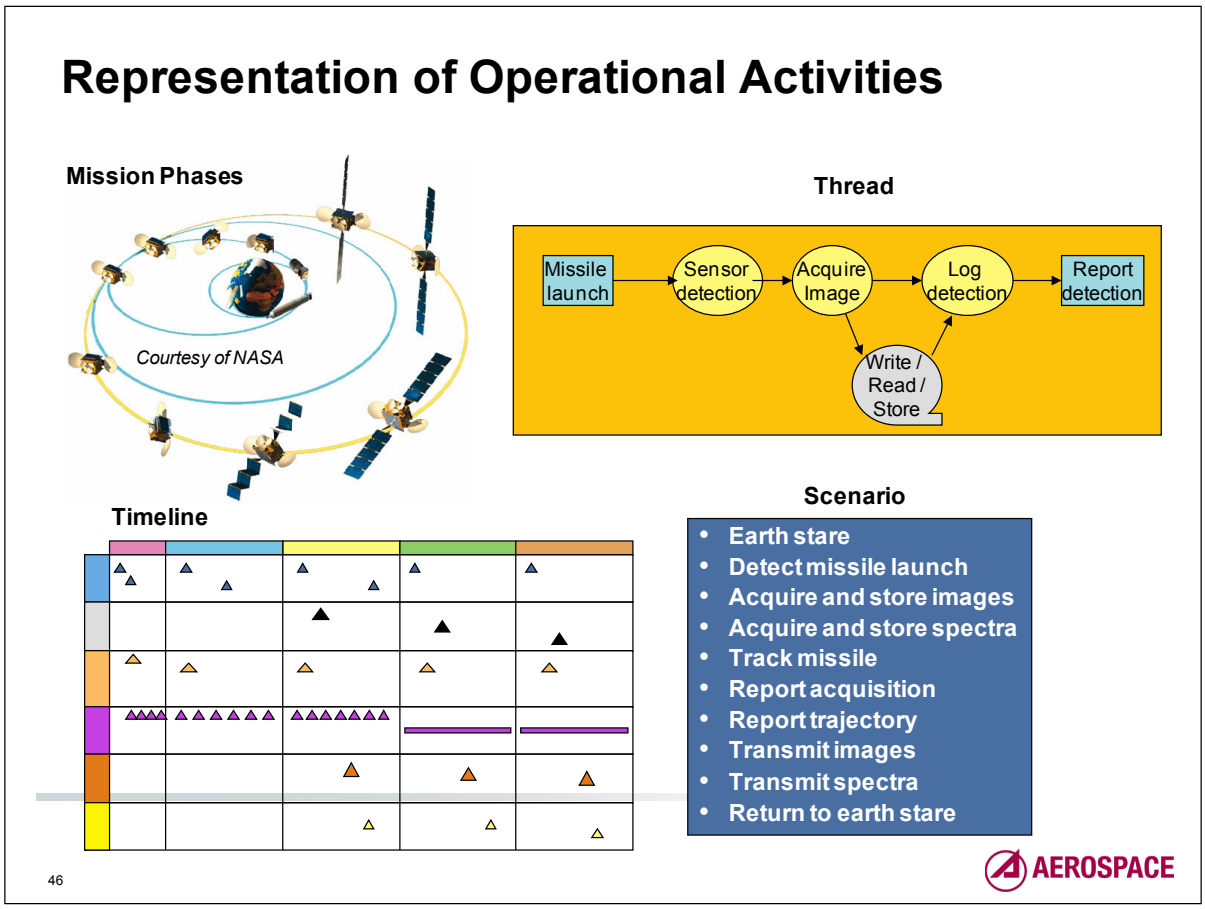
45

AEROSPACE

Every mission will want to consider these activities, from the top of the function pyramid, for candidate LYF tests. Where specific events, such as solar array deployment, cannot be included at the higher integration level, later steps will describe the process for allocating the activity to testing at a lower level of integration.

LYF tests for fault management and contingencies require careful consideration. It is critical for mission safety that the vehicle's fault responses execute as expected and that the recovery procedures are sound. In this step of the TLYF process, critical fault management and recovery events must be identified and the appropriate "ends" defined. Fault management tests might need to include ground recovery activities. Contingency tests should not only include SV anomalies, but also ground system anomalies. If those involve failover to alternate ground facility, the back-up facility will be one of the "ends" of the tests. Later steps will address the mechanisms that might be needed to conduct such tests of fault situations.

Slide 46




This chart provides an example of the levels of the function pyramid, applied to the specific example of a missile detection system. At the Identification step, the LYF candidates will be from the mission phase and timeline levels.

A **thread** for this example could be the verification of the missile detection capability. This would include the ability for the sensor to respond to an input stimulus that: (1) emulates a missile launch, (2) translate that into an image, (3) have the data handling system write/store the image, (4) log a detection (perhaps increment a detection counter) in a state of health parameter, and (5) produce a detection report (output for a follow-on function or thread).

A **scenario** for this example is the detection and tracking of a missile launch with a return to the initial, quiescent stare, condition of the vehicle. This is the basic "mission" scenario of the satellite.

A **timeline level of test** would include a representative set of activities that would be performed by the vehicle and ground segment over the course of a few days. This would include: (1) automated spacecraft and payload activities, (2) execution of the mission planning activities to produce a schedule and commands to be uploaded to the vehicle, (3) uploading commands as appropriate to vehicle contact times, (4) insertion of "missile launch events" for the vehicle to detect and transmit, (5) recovery of vehicle state of health and mission data, and (6) mission product generation.

A **mission phase test** would include all, most, or some of each mission phase, depending on the duration of the phase and the ability to emulate key mission phase objectives. It should be possible to include a test of the complete "ascent" phase. It should be feasible to perform most, if not all, of an

orbit transfer phase. Nominal operations, which comprise the bulk of the mission, should have an appropriate long (days, weeks) selection covering as many types of activities/scenarios as feasible.

Slide 47

## Mission Phases and End-to-End Configurations

| Mission Phase | Timeline | End-to-End Configuration |
|---|---|---|
| Ascent | T+0 through LV Separation | SV + LV (+ LV Range) |
| Automated Initialization | LV Separation through first planned ground segment commanding | SV |
| Orbit Transfer | First post sep orbit determination until final orbit achieved (may overlap SV commissioning) | SV + Ground command and control segment (GS) + JSPOC |
| SV Commissioning | First planned ground segment commanding through ready for ops | SV + GS<br>SV+GS+ user facilities in late stages |
| Normal Ops | Ready for ops through special ops or End of life (EOL) | SV + GS+ user facilities (tasking and mission data processing) |
| Fault and Contingency | Any applicable mission phase | SV or SV + GS |

47

AEROSPACE

When exploring LYF test options, it is necessary to consider more than the "nominal" operations activities.

This table provides a starting point for identifying the "other" phases and provides an indication of where they lie on a full mission timeline.

It also highlights the end-to-end points for each phase that need to be considered/included for LYF testing. Some fault and contingency responses may need to include user systems.

Slide 48

## Candidate LYF Tests

### *Depend on Supplier Level Perspective*

- LV Integrator
  - *Ascent phase test of the integrated LV*
- SV Integrator
  - *Ascent phase test of the integrated SV*
- Range Integrator
  - *Ascent phase test of the integrated range*
- LV/SV/Range Integrator
  - *Ascent phase test of the integrated LV/SV stack + range*
  - *Ascent phase test of the integrated LV/SV stack*


Courtesy of NASA


Courtesy of USAF


Courtesy of NASA

*Questions to ask:*

*Who is doing the test (supplier) and what the stated mission objectives are for that supplier?*

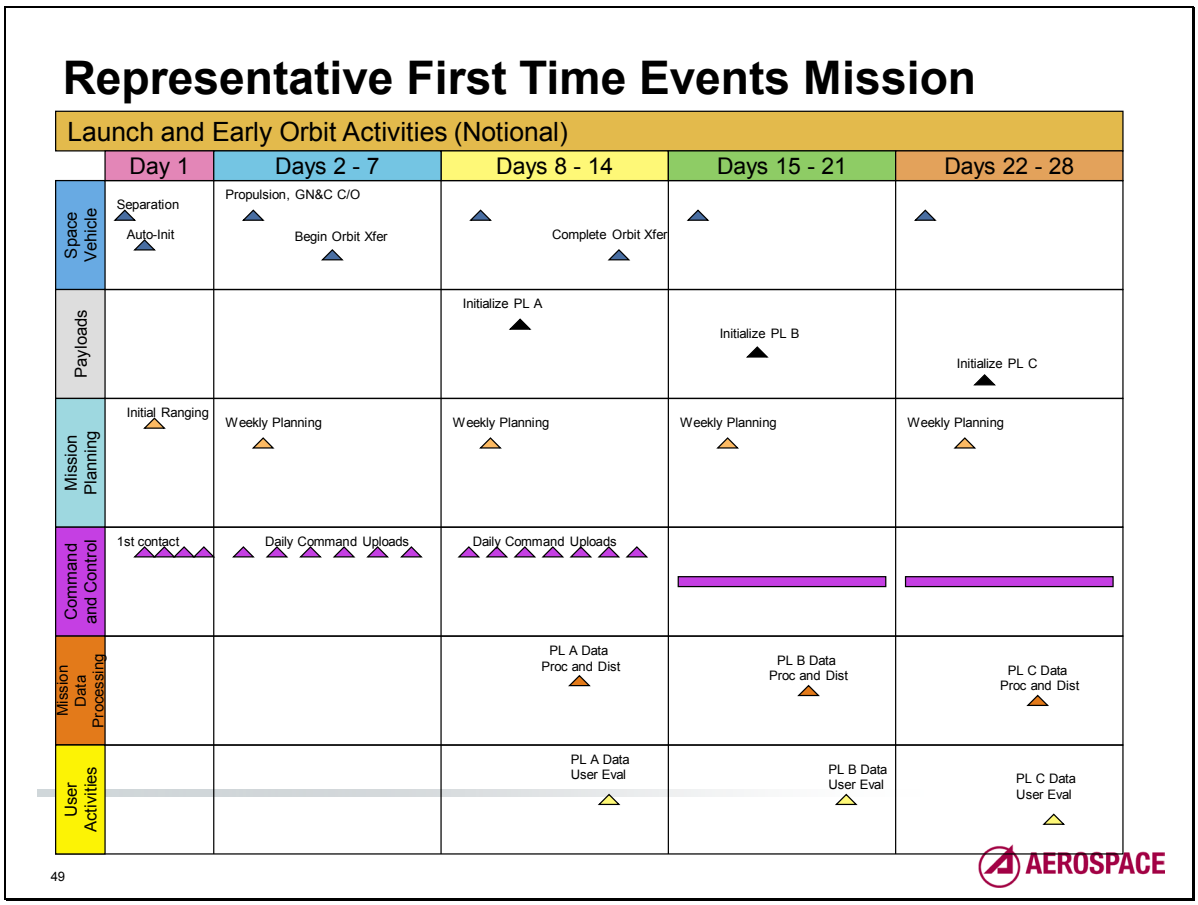
48

AEROSPACE

We have been concentrating on the view of the system integrator. However, appropriate LYF tests depend on perspective. Ascent is an illustrative example because three major organizations/systems—launch vehicle, space vehicle, and range—are involved. Different contracts for the different integrators will result in different LYF tests, possibly with different objectives, even for the same mission phase.

We will return to this in discussing the allocation of LYF tests.

Slide 49

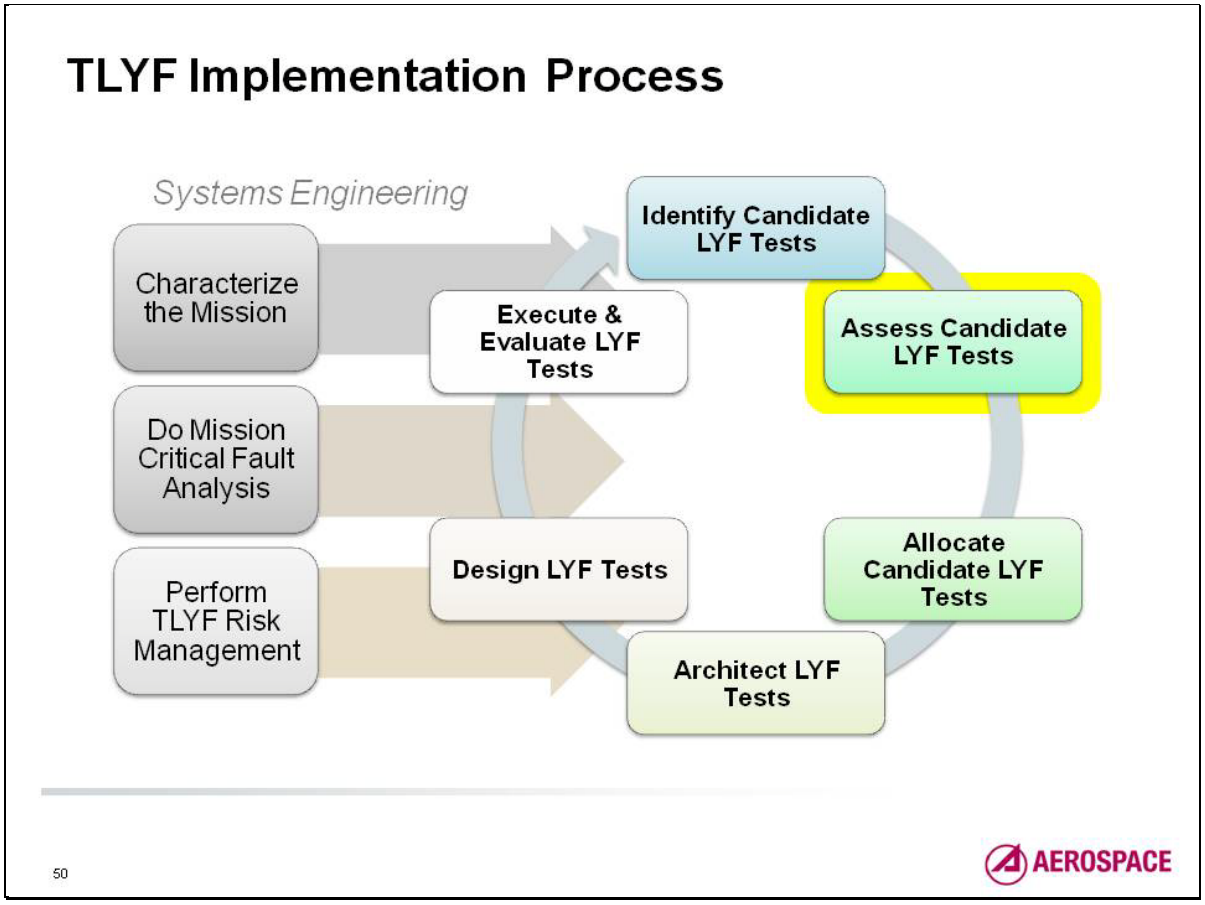



Given that the fundamental principle of TLYF is to perform activities for the first time pre-launch rather than during the actual mission, it follows that we must be cognizant of what those "first time" activities are. A "first-time" activity is not only the literal first time a discrete activity is performed, but is also the first time a repetitive set of activities (e.g., "nominal ops") is performed. Both versions of a first time activity are needed as the basis for the "days-in-the-life" (DITL) tests, with the second version necessary to flush out accumulation and asynchronous timing errors that need more than a single occurrence to allow these kind of flaws to manifest.

We also use the concept of "mission critical" activities as a foundation for the later subject of fault analysis of mission critical situations. A mission critical activity is one that must be successful in order to accomplish, or be able to accomplish, the primary mission objective(s). In some phases, particularly early phases, almost every activity is "mission critical." In other phases, there may be many "first time" activities that are themselves not mission critical, but which must be executed in flight order to provide the appropriate initial or transition mission conditions for mission critical activities.

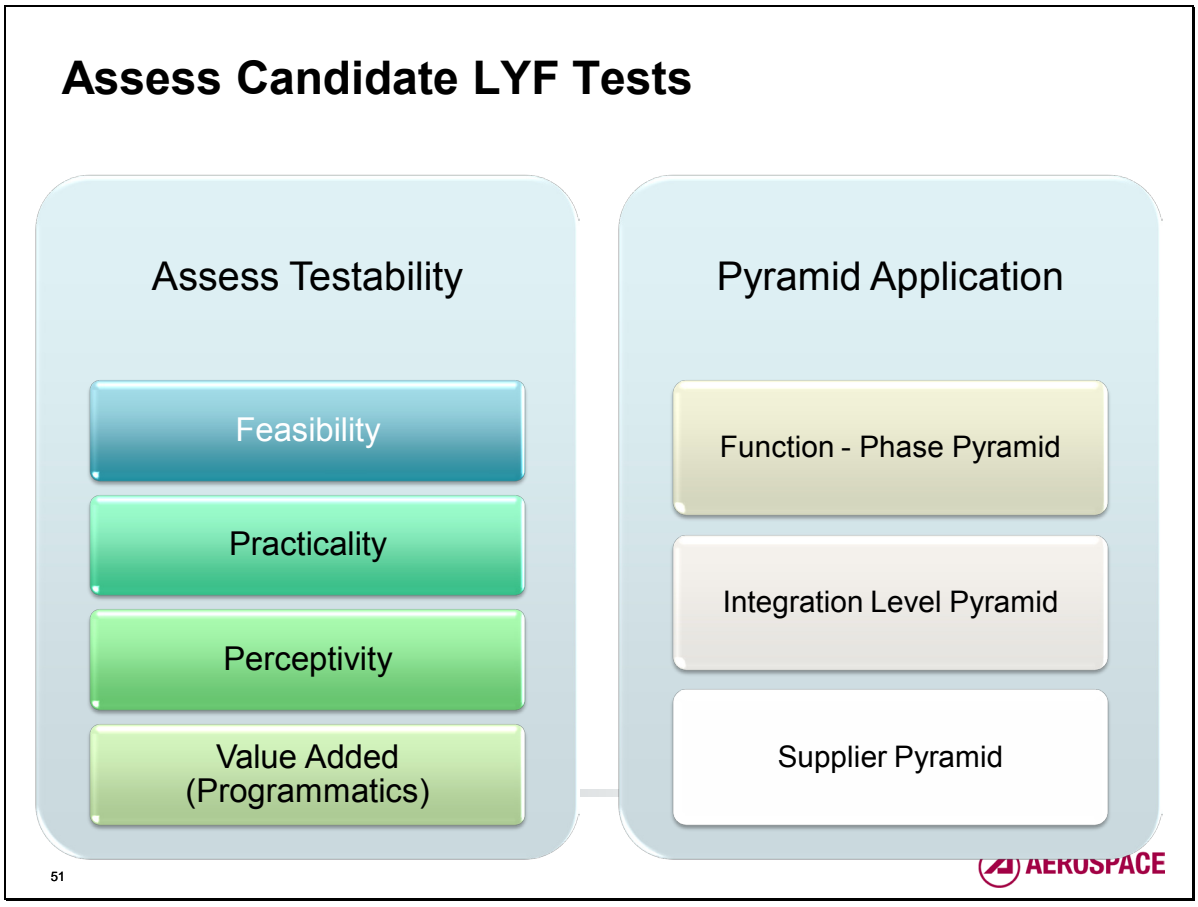
The "first time analysis" (FTA) is an iterative process that can be initially performed following the development of the mission concept of operations. This initial analysis may just help define the mission phases and the key activities within those phases. As more detail becomes known during the development phases, the FTA should be updated. The purpose of the FTA is to provide the completion criteria for a TLYF assessment. It is also the basis for allocating activities to the LYF tests. Each first time activity either needs to be included in some appropriate level of integrated test, or accounted for in the TLYF exceptions analysis.

Slide 50




The next step in the process is to assess the candidate tests as to the feasibility, practicality, and perceptiveness of the test at the highest levels of function and integration.

Slide 51




This step focuses on the whether each of the candidate tests, performed at the highest relevant level of function and integration, is feasible, practical, and perceptive to flaws. The value-added criterion addresses the cost/benefit of a particular test.

Where it is not feasible or practical to perform the test at the highest level of the function and integration pyramid, or if a test performed at that level is not perceptive to some class of critical flaws, the engineer will identify the appropriate levels to perform the test.

Slide 52

## Assess LYF Candidate Tests

- Description:
  - *Assess testability of each LYF candidate for feasibility, practicality, perceptivity, and programmatic value at the highest applicable level of integration to determine how much of the system should be tested at that level.*
  - *Assess candidates for testability at lower levels of the integration, functional, and supplier pyramids as necessary for risk reduction, practicality, or better perceptivity.*
    - Assessments must be in context of mission objectives and associated applicable mission characteristics.
- When used:
  - *Pre-RFP: Used at a high level to identify/scope the resources that the program will require specifically for LYF tests.*
  - *For SRR: Initial plan for test allocation*
  - *For PDR: Updated, especially to include allocations to the supplier pyramid*
  - *For CDR: Updated to account for design changes*
  - *After CDR: Updated to account for re-design*

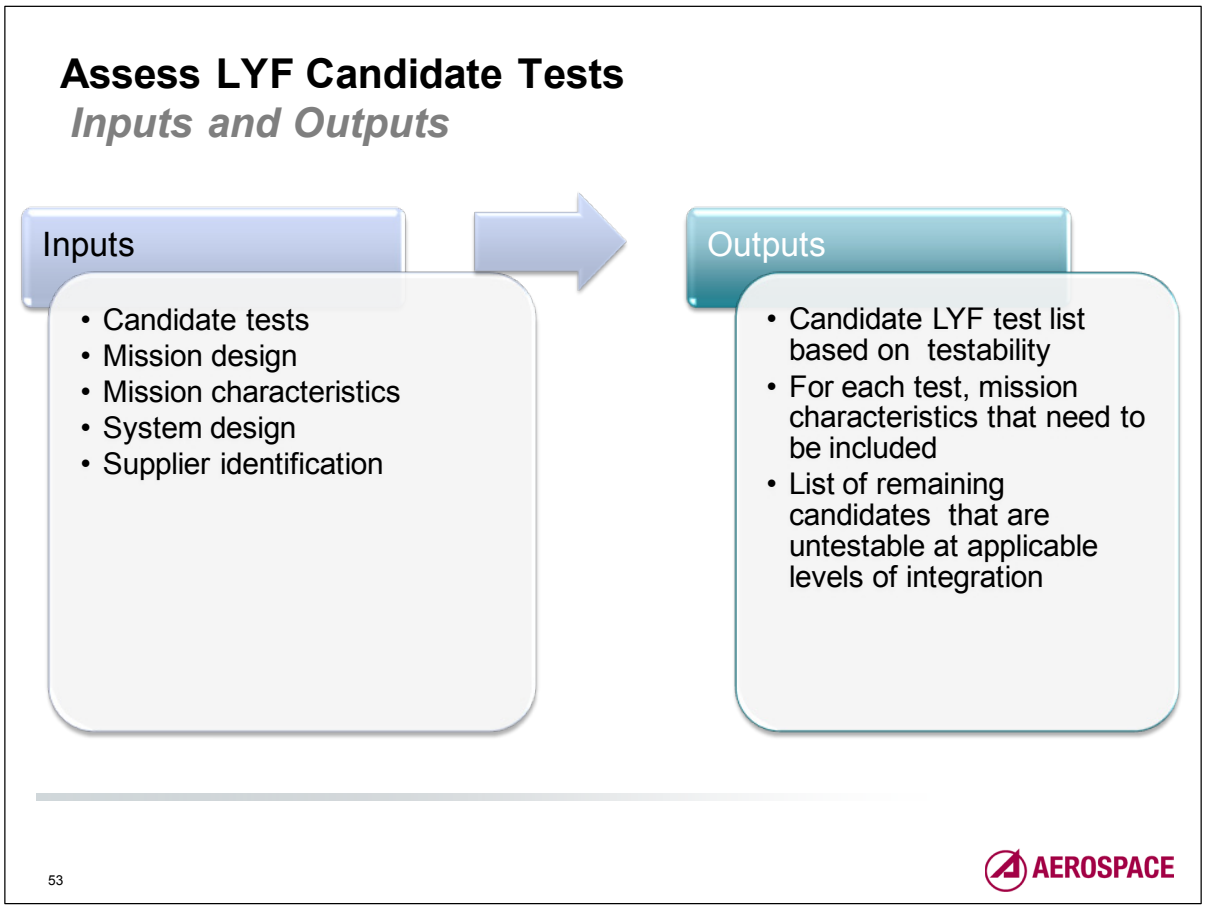
52

AEROSPACE

The program office must first perform this step to scope the effort appropriately for program planning and to properly specify TLYF requirements in the RFP. The next slide discusses how LYF testing can affect program schedules.

This step must be revisited as the design matures, as specific design decisions may affect the feasibility of a test at a particular integration level.

Slide 53




At this step, the physical conditions of the test are being defined. For instance, for a TOCT for a sensor mission, the output of this step might include the following characteristics in the test:

- Integrated SV with mature S/W
- Scene stimulator
- User participation (receive tasking files for upload to vehicle, distribute data to mission processing)
- TVAC – run through two temp cycles representative of on-orbit conditions
- Ground system with mature S/W
- Operator participation – use ops procedures
- Run operational timeline for 72 hours, no time compression

Note that this test, requiring that the SV and ground system have mature S/W, and using operational procedures, has schedule implications. TVAC testing is frequently done before S/W is mature, but the TOCT would not provide mission validation at that point because of the "Test What You Fly" violation.

For SV fault conditions, there may be situations in which it is infeasible or too risky to induce the fault on the vehicle. In these cases, a “flat sat” running mature flight software on flight identical processors, with simulated subsystems, may be the choice for LYF testing. The limitations of this arrangement must be clearly understood and appropriate validation of the “flat sat” conducted.

Untestable candidates will usually be specific events within a larger sequence of events. For instance, physical solar array deployment may not be testable within the automatic SV initialization. It would then be a candidate for testing at a lower level of integration.

Slide 54

## Testability: Feasibility / Practicality / Perceptivity

- The concept of "testability" is to provide an assessment of the **fullest practical extent** to which the literal mission can be translated into test
  - *It accounts for the physical and engineering limitations, and balances what can be done in a flight-like manner with acceptable and understood risk and program constraints.*
- Feasibility assessment
  - *Which of the necessary applicable concurrent attributes does physics allow?*
- Practicality assessment
  - *How much of what theoretically could be done is practical from an engineering perspective?*
- Perceptivity assessment
  - *Can the test reveal flaw types appropriate to the integration and functional level of the test?*
- Programmatic value assessment
  - *Cost/benefit/risk*
- How do the answers change as a function of each pyramid level?

54

AEROSPACE

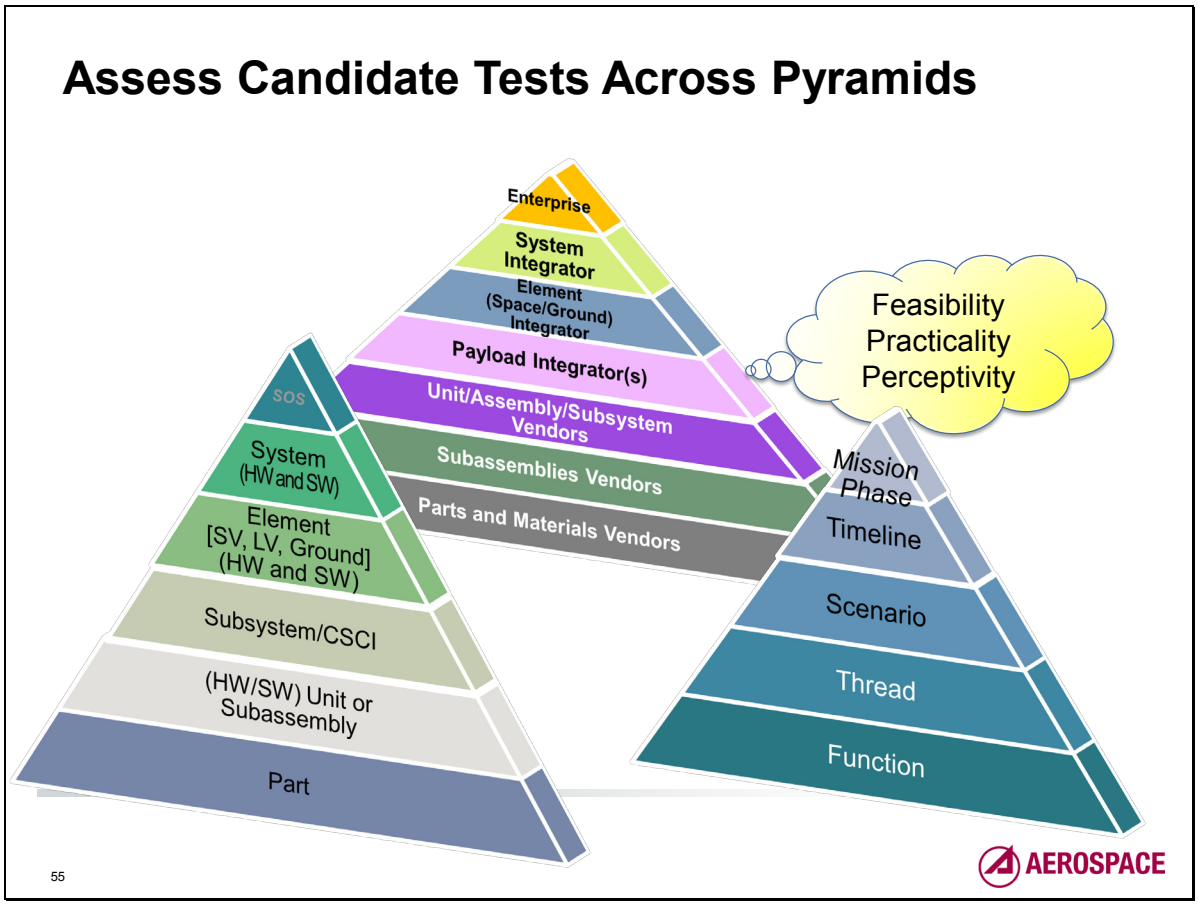
This step is where the ideal of "fly the mission on the ground" meets the realities of physics and engineering. For example, the EMI/EMC environment may be critical to performance for a given mission. Simulating that environment may not be possible with other flight-like environments. It may be most perceptive to run a normal operations timeline involving active transmitters in the EMI/EMC environment.

The ascent portion of a mission involves a number of computer processors, sensors and RF equipment operating according to algorithms and pre-programmed commands in a rapidly changing vibroacoustics environment induced by the launch vehicle concurrent with decreasing atmospheric pressure and temperature, punctuated by several shock events. It may be technically feasible to create a test facility and associated set of equipment to emulate the whole ascent combined environments profile for the full time between launch (T+0) through vehicle separation for a space vehicle, but there are likely to be numerous issues related to practicality, perceptivity, and programmatic value. The assessment might be quite different for a space vehicle that is an unmanned free-flyer with much in common with other free flyers tested in traditional ways than for a new manned crew vehicle. It may be that the most practical test of the timeline is one that involves the processors and sensors in a single environment.

It is not likely to be feasible to perform an automated initialization of a spacecraft in a vacuum environment that includes deployment of large solar arrays, but it may be very feasible to do the automated initialization without the actual deployment (a TLYF exception). It would then be necessary to perform the deployment in some other setting, with or without the vehicle. If done

without the vehicle, this would be considered to be at the assembly level of integration, possibly as a deployment “thread.”

Slide 55




So far, we have discussed the point of view of the system integrator. However, the system integrator may levy LYF testing requirements on the suppliers. In doing so, the system integrator must ensure that the supplier understands the conditions of use of the subsystem or component and that the LYF testing is able to replicate those conditions. Besides environmental conditions, timing and circuit response characteristics may be among the critical conditions that need to be replicated for a LYF test.

Slide 56

# Mission Phases, End-to-End Configurations and Candidate LYF Tests

| Mission Phase | Timeline | End-to-End Configuration | LYF Test | LYF Test Venue |
|---|---|---|---|---|
| Ascent | T+0 through LV Separation | SV + LV (+ LV Range) | SV Ascent with LV simulated inputs | SV Factory (ambient or begin TVAC) |
| Automated Initialization | LV Separation through 1st planned ground segment commanding | SV | SV auto init with LV simulated sep signal, … | SV Factory TVAC |
| Orbit Transfer | 1st post sep orbit determination until final orbit (may overlap SV Commissioning) | SV + Ground command and control segment (GS) + JSPOC | Orbit transfer interactions test (no propulsion) | SV (+ simulators) + GS + JSPOC |
| SV Commis-sioning | 1st planned ground segment commanding through ready for ops | SV + GS | Entire commissioning timeline, with some time compression | SV Factory TV + GS |
| Normal Ops | Ready for ops through special ops or EOL | SV + GS + user facilities (tasking and mission data processing) | Normal ops on representative timeline for 120 hours | SV Factory TV + GS + user facilities |
| Fault and Contingency | Any applicable mission phase | SV or SV + GS | Applicable ops with transition into fault handling and recovery | Factory Flatsat + GS |

56

This chart is a notional assessment of how a program might start to define feasible LYF tests. As the tests are identified, the facilities and special equipment needed are also defined.

JSPOC – Joint Space Operations Center

Slide 57

# Example: Assess Ascent First Time and Mission Critical Events and Activities

Ascent (Space Vehicle)

| Timeline | Critical Event |
|---|---|
| Prelaunch | Spacecraft computer unit (SCU) |
| | Database upload |
| | SW patch upload |
| | Initialize configuration for launch |
| | Switch to internal power |
| T + 0 | Launch signal for SCU timer |
| T + 837 sec | Turn on SGLS transmitters |
| T + 58 min | Separation |

Ascent (Launch Vehicle)

| Timeline | Critical Event |
|---|---|
| Prelaunch | Initialize configuration for launch |
| T + 0 | Liftoff |
| T + 82.5 sec | GEM jettison |
| T + 264 sec | Main Engine Cutoff |
| T + 277.5 sec | Second stage ignition |
| T + 281.5 sec | Fairing jettison |
| T + 685.1 sec | Secondary Engine Cutoff |
| T + 58 min | Separation |

57

AEROSPACE

The next three charts present an example of the ascent mission phase.

From the SV point of view, there are two critical events: receipt of the launch signal to start the SCU time and turn-on of SGLS transmitters. Besides these two events, the critical thing for the SV is surviving the launch environments.

The LV performs a complex series of actions during ascent.

From these critical events, feasible and perceptive LYF tests at the SV and vehicle level must be derived.

Slide 58

## Example - Assessing Ascent Phase Testability: What Mission Objectives Are To Be Included?

- Supplier Perspective
  - *Launch Vehicle Supplier*
    - Achieving mission orbit
    - Maintain integrity of payload
  - *Space Vehicle Supplier*
    - Appropriately perform ascent events and activities
    - Be ready to conduct space vehicle activities after separation
- Feasibility
  - *Is it possible to test the planned flight profile at the appropriate level of integration?*
- Practicality
  - *Engineering test implications*
- Perceptivity
  - *What kind of flaws can be found?*
- Value
  - *What will we learn from this test that we won't learn elsewhere*

58

AEROSPACE

The ultimate pre-launch execution of a launch vehicle mission would involve all LV subsystems executing according to the ascent timeline. One can envision a fully loaded (propellant) rocket stage tied down on a test stand for a "hot fire" test. This is not only practical, but has been done. What is probably not feasible is to perform a hot fire test in a chamber that dynamically adjusts temperature and pressure to emulate those environments over the stage timeline. For a single stage rocket, all that would be needed to be a more practical LYF test would be the addition of a payload and fairing for demonstrating separation events. It would probably be feasible, but not be practical, to actually eject the fairing and payload. It would be practical to have electrical simulators as stand-ins for those articles. It would then be necessary to assess differences to the mission (delta pressure, delta temperature, and simulators) for potential flaw escapes.

Different tests will be perceptive to different kinds of flaws. Tests involving physical propulsion hardware loaded with mission-applicable fluids can be perceptive to flaws relating to fluid flow hardware design/workmanship and hardware/software interactions concerning control algorithms, physical control, and sensing. Tests involving ground planning software, ground data evaluation software, and flight software can be perceptive to algorithm mismatches and other potential software flaws (units, sign direction, and processing issues).

The launch vehicle scenario becomes much less feasible when considering a multistage rocket. From a practical perspective, each stage can be tested separately as above, with a separate timeline test of the software/electrical/mechanical integrated elements.

Slide 59

## Exercise: Assessing SV Ascent Phase Testability

*What Key Characteristics Must Be Included?*

- How close can we come to flight?
  - *We have a few acoustic chambers with vibration tables*
  - *What SW version?*
  - *We have a large number of thermal-vacuum chambers, but few if any that can decrease both pressure and temperature on ascent timescales for most SVs*
  - *RF??*
- How close do we need to come to flight?
- Timeline
  - *Sequence*
- Continuous clock from T-?? to T+ ??
- Dynamically changing combined environments?
  - *Vibroacoustics, shock, RF, thermal, atmospheric pressure*
- Other characteristics?

***What Do You Really Need to Test?***

59

AEROSPACE

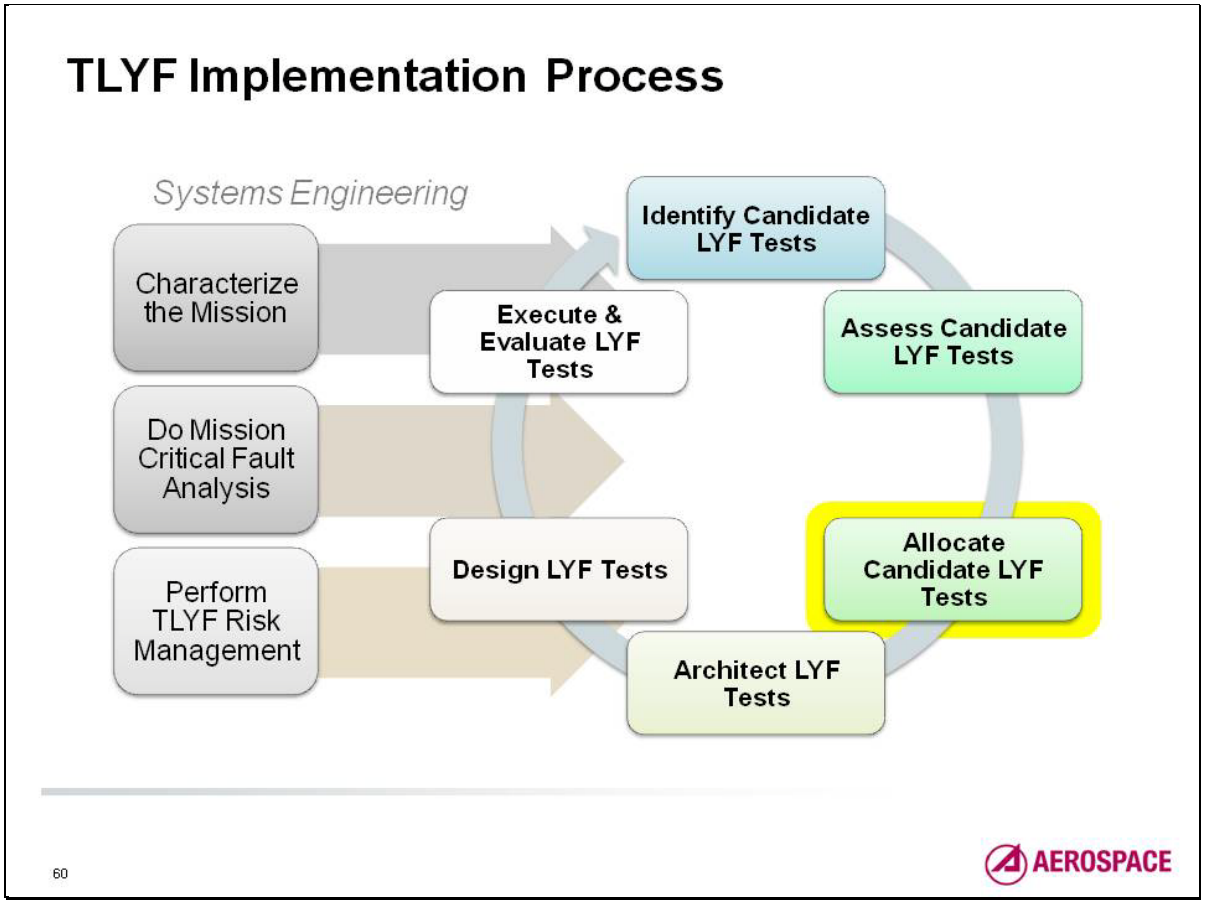
What goes on during any mission phase may be reasonably well known, but the thought process for determining what should be translated into test is not as well defined. The thought exercise of examining the ascent phase from the space vehicle test perspective should help establish the kinds of considerations to examine in the translation from mission to test.

Ascent on most launch vehicles is accomplished in a series of active events from initial ignition of the first stage through the separation of the SV from the booster, as shown in the previous tables. The most straightforward translation of what the SV is doing is derived from the SV software/firmware/sensor activities. For free-flying satellites these are generally assessing the time from launch to initiate clock-driven SV activities (e.g., turning something on or off), interpreting internal sensor and fault management information (did a watchdog timer time out?), or acting on an external signal (separation). Whatever the SV is doing during the ascent phase it is also experiencing a changing set of environments induced by the LV (vibration, shock, RF), and due to the change of altitude (temperature, pressure). Does all this mean we must do an ascent phase test of the SV executing its logic in the presence of the combined environments to be truly "like you fly"? If we don't do that combined environments ascent timeline test, how must we account for all the exceptions to the actual ascent phase?

In the early days of spacecraft development, a number of satellite providers did some very elaborate tests that could be considered LYF tests. The most common of these was to put the qualification or first entire vehicle on an air-bearing table primarily to exercise and validate the guidance, navigation, and control subsystem performance. We don't do those kinds of tests today for our "normal" free-flying satellites because we have developed alternative methods for such validation. One thing we

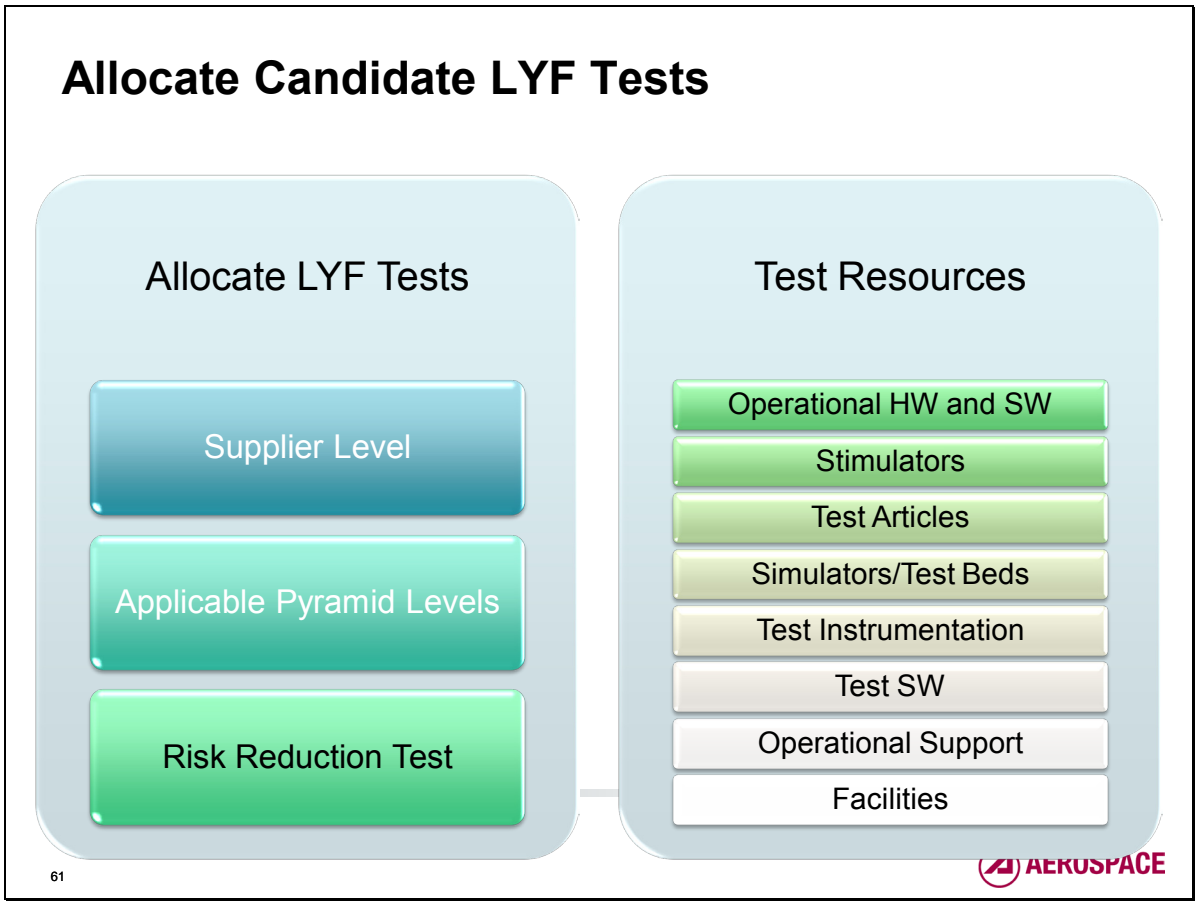
have learned is that we can get good value by bounding the environment effects and applying them to design verification and workmanship screening tests, especially at the unit and higher levels of integration. We do not have a body of evidence to suggest that we are letting mission-critical flaws escape to orbit by using the non-LYF, serial environment test techniques prescribed in MIL-STD-1540 at those levels of integration. We do have evidence that the lack of timeline testing of SV logic has allowed such mission-critical flaw escapes.

Slide 60




This step allocates the candidate test to a specific integration and function level, and to specific test resources. The output of this step are the LYF tests that the program plans to do, allocated to appropriate levels of the function, integration, and supplier pyramids. For each test, the needed test resources are also identified.

Slide 61




As will be discussed in more detail in a later chart, Like You Fly testing at lower levels of the integration and function pyramids can provide risk reduction by catching problems early, when the costs of remediation will be lower. So even if the final validation will be provided with a high-level test like the TOCT, the program should evaluate the cost/benefit of LYF testing at lower levels, or earlier stages of development.

Although a prime tenet of TLYF is to test "What You Fly," this may not always be possible. In evaluating test resources, use of non-flight articles should be closely scrutinized. Test resources must also be evaluated for availability. In order to successfully perform LYF tests, operational support resources must be available. Historically, ops development (ground system availability, personnel training, and ops procedure development) has lagged SV development. In allocating test resources, the program must track the development of those resources to ensure that they are available when needed.

Slide 62

## Allocate LYF Candidate Tests

- Description:
  - *Allocate LYF candidate tests to applicable levels of the integration, function – phase, and supplier pyramids as indicated by the assessment.*
    - Allocation should indicate what mission objectives and characteristics are included.
  - *Determine and allocate the resources required for this testing.*
- When used:
  - *Pre-RFP: Used at a high level to identify/scope the resources that the program will require specifically for LYF tests.*
  - *For SRR: Initial plan for test allocation*
  - *For PDR: Updated, especially to include allocations to the supplier pyramid*
  - *For CDR: Updated to account for design changes*
  - *After CDR: Updated to account for re-design*

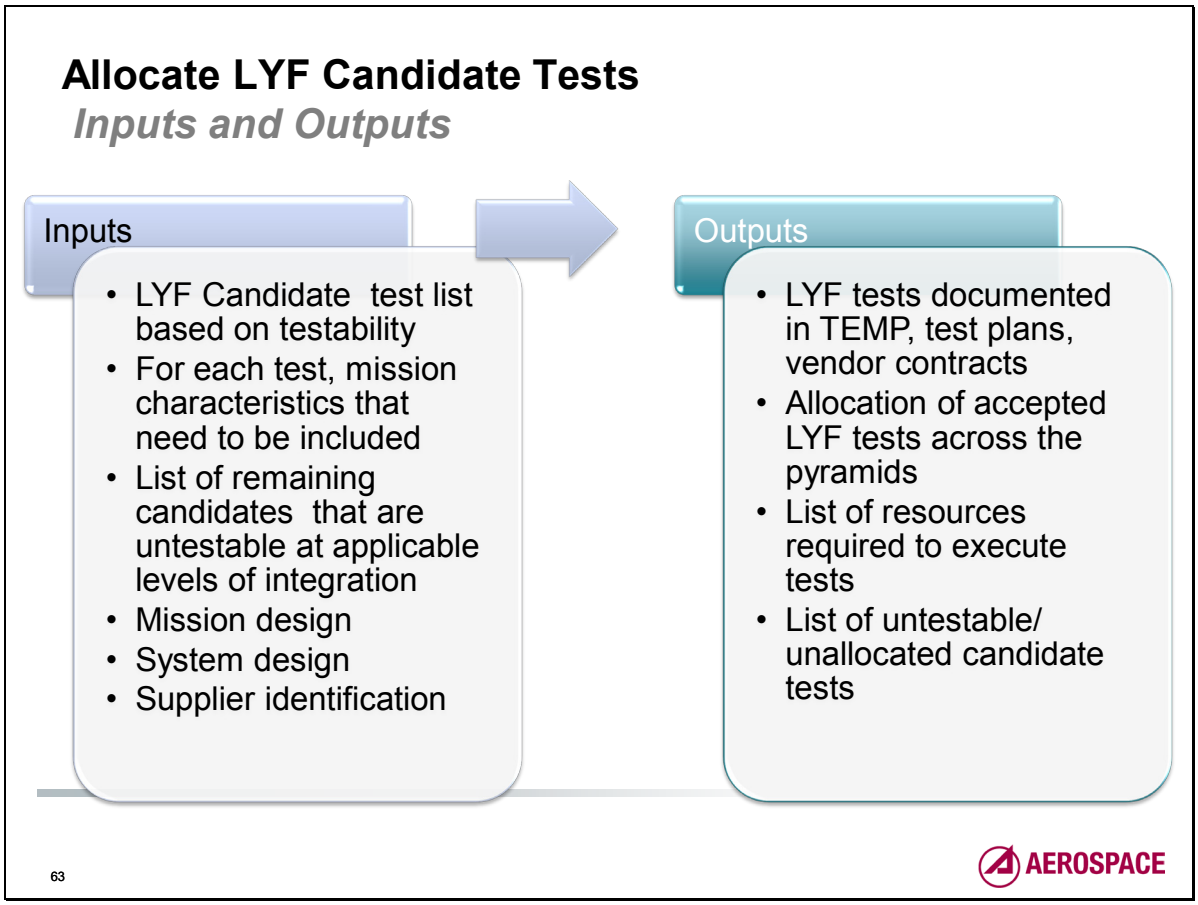
62

AEROSPACE

The output of this step will enable the program office to plan for appropriate resources and provide a schedule and budget for the TLYF effort. It will also ensure that the TLYF requirements in the RFP reflect the program office intent.

At SRR, whichever organization will be responsible for the LYF testing provides the initial plan. Because the LYF tests potentially span organizations (e.g., ground system developer, SV developer, and LV integrator), the overall responsibility may rest with the system integrator. As the design matures, this plan must be updated to reflect the testing each supplier will be providing and to reflect design and CONOPS changes.

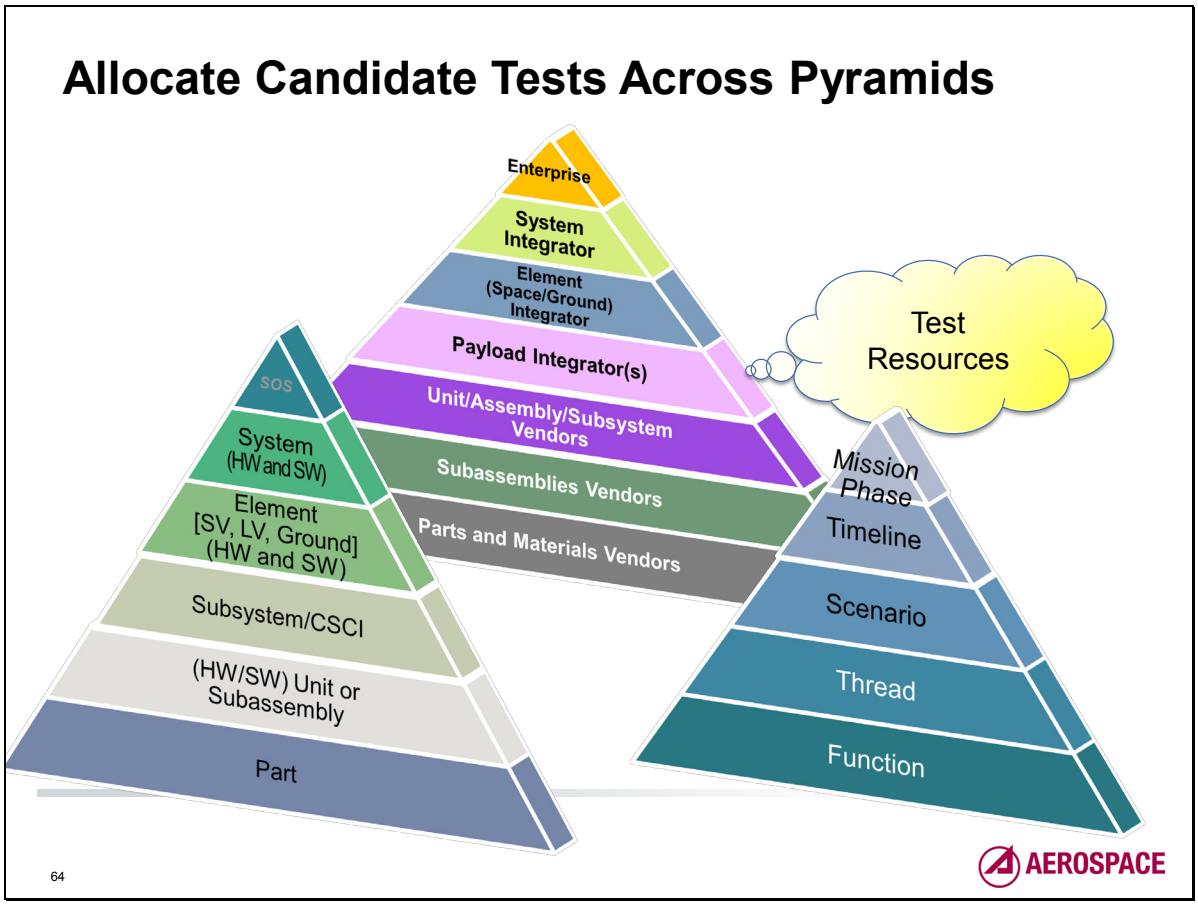
Slide 63




The output of this step is the LYF tests that will be performed. As the program proceeds with development, these tests are documented appropriately: in the RFP, in the TEMP, in vendor contracts, and in test plans.

Candidate tests that were deemed untestable and were therefore not allocated to any test must be documented as LYF exceptions and evaluated in the next step, Critical Fault Analysis.

Slide 64



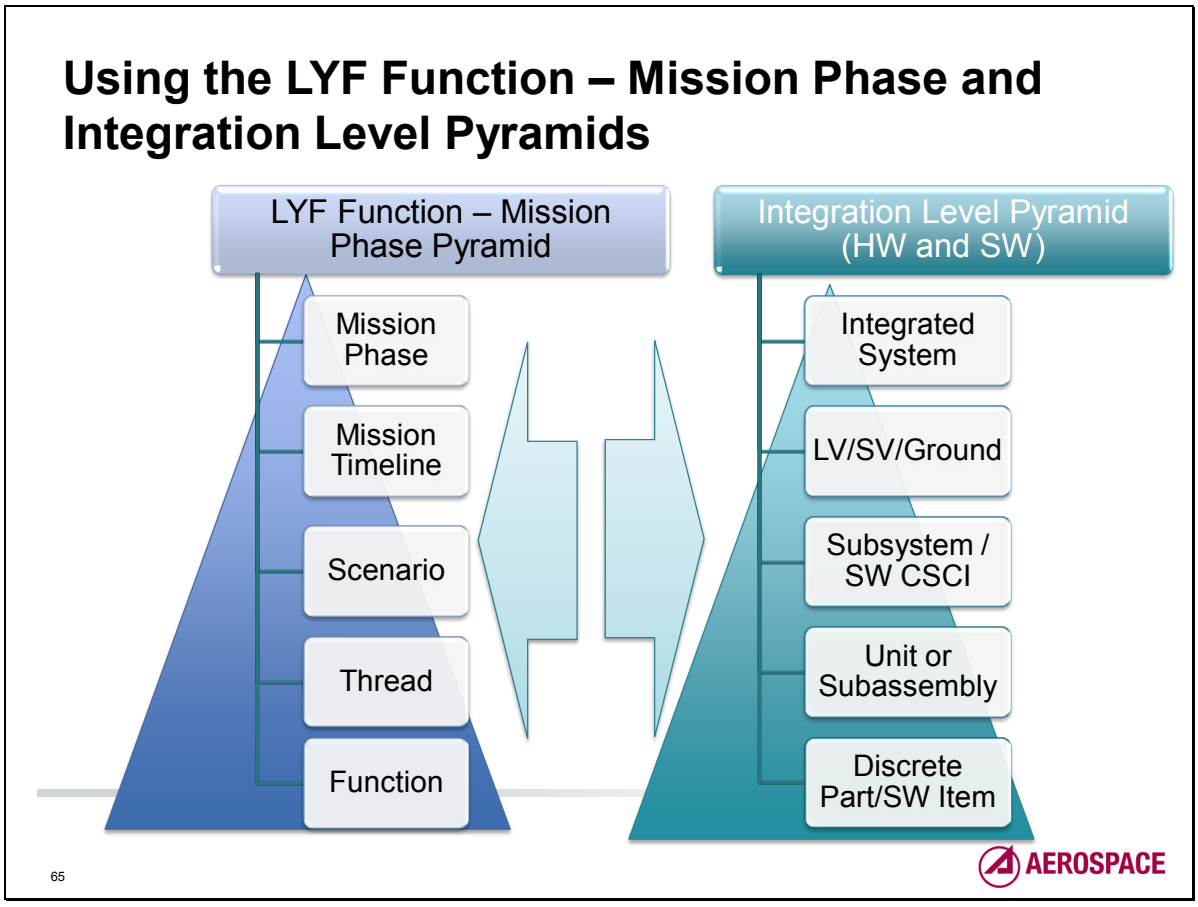

The driving motivation for beginning the TLYF approach at the start of the program is to be able to allocate LYF tests at all appropriate levels of development and integration. As powerful as the TOCT is at revealing system (and item) flaws, there will always be mission critical- and first-time events that cannot be adequately or safely performed at this level of integration. It is very late in the flow to be finding flaws that are fully contained and observable at much lower levels of integration. There are also flaws that cannot be perceived at this level of integration.

There are two paths that need to be considered for allocating LYF tests to lower levels of integration: the path within an acquisition program's direct control via contract, and an early path for externally provided items.

A LYF test at higher levels of integration (payload, SV, integrated launch vehicle, space segment + ground segment, and full system of systems) should execute a complete mission phase or several mission phases with phase transitions. A LYF test at lower levels of integration (part, unit, subassembly, subsystem), should execute a portion of a mission appropriate to the item under test.

There are two reasons to do "like you fly" (LYF) tests at lower levels of integration. The first is to adhere to the pyramid test philosophy so that flaws can be found at the lowest, and cheapest level. The second reason is that many mission activities are not possible or practical to test at the fully integrated system or vehicle level.

Slide 65




Some mission activities are not feasible at the highest appropriate levels of the function and integration pyramids. For example, a common activity done by the SV after separation from the booster is an autonomous deployment of its solar array, orienting the array to the sun, and establishing a positive power condition. The highest level of integration as a first time activity is the SV. There are likely to be potential critical flaws that might only manifest under certain thermal conditions, and some flaws that will only surface in a vacuum. However, for most deployable solar arrays it would not be feasible to execute a deployment within the confines of a thermal or thermal-vacuum chamber. It may be possible to deploy solar arrays attached to the SV in an ambient environment, but there may be safety concerns or other risk concerns for the solar array itself or for other aspects of the SV. Thus, it may be prudent to allocate LYF risk reduction tests to the subassembly (solar array) level, and to the subsystem (power, flight software) level. If the solar array uses a new technology/material for the cells or panels, it may be necessary to allocate a test of a part or subassembly to a combined environment (thermal, vacuum, and radiation) test.

What equivalent thought process would we use for allocating LYF tests to the function pyramid? If the deployment of a solar array is part of an "autonomous initialization" mission phase, then a LYF test should be allocated to a mission phase test. It may be prudent to do a mission timeline LYF test that only includes the series of activities of solar array deployment through orienting the array to the sun, and ending with power distribution from the arrays to the power subsystem. Lower level risk reduction tests may be allocated to an array deployment scenario, a scenario for orienting the array (and SV) to the sun, and a thread to follow incident energy on the solar array through to the power distribution system.

How do we combine the function pyramid allocations with the integration level pyramid? It may be that it is not feasible to execute that entire mission phase with the actual vehicle. It may be feasible to do a mission timeline LYF test that only includes a limited series of activities, e.g., solar array deployment through orienting the array to the sun. If that is not feasible, or if it's prudent to perform a lower level risk reduction test, a deployment thread (command through first physical motion of the solar array assembly) may be planned.

Slide 66

## Allocating Candidate LYF Tests to Resources

- Sensor Stimulators
- Engineering Units
- Space Vehicle Simulators
- Substitutes for Ground Elements
- Test Beds
- Test Instrumentation
- Factory Test Control Hardware
- Factory Test Software and Databases
- Test Procedures and Other Ground Test Documentation
- Test Personnel
- Facilities

- Operational HW and SW
- Ground Control Equipment
- Operational Support
- Operational Procedures
- Facilities

***Some candidate LYF tests can and should be allocated to appropriate test resources (e.g., test bed, simulator/ simulation) primarily for some sort of risk reduction***

66

AEROSPACE

Continuing the example of the SV autonomous initialization mission phase, there are key characteristics from the mission that are not available in a factory environment, and there are some activities that are not feasible or not practical on the flight equipment at any level of integration. This is a primary consideration for the necessity to utilize and allocate candidate LYF tests to test resources.

A solar array needs to see something that looks like sunlight to validate that it can transform the incident energy into power. It may be feasible and practical for some arrays to be taken out of a building and exposed to direct sunlight, but most flight hardware will need to be protected from the ambient environment. A risk reduction LYF test of the energy transformation thread may be allocated to an engineering version of the solar array and associated power subsystem hardware, exposing non-flight hardware to the sun in an outdoor ambient environment. Alternatively, the actual flight hardware may be exposed to a solar simulator, which will stimulate the solar cells in the appropriate wavelength range with an approximation of solar energy.

At some point in a test program of an autonomous system, a contingency should be exercised. In the case of the solar array deployment example, a failure to deploy can be a mission-ending situation that may be recovered by quick and appropriate action by the ground control team. A solar array deployment failure contingency test will need to be allocated to a combination of actual hardware, test beds, and simulators. The allocation has to further consider whether it will be done with the actual ground control equipment, processes, and personnel. Would there need to be a risk reduction allocation to test control equipment and personnel?

Slide 67

## Reasons for Allocating Candidate LYF Tests to Specific Levels in the Pyramids

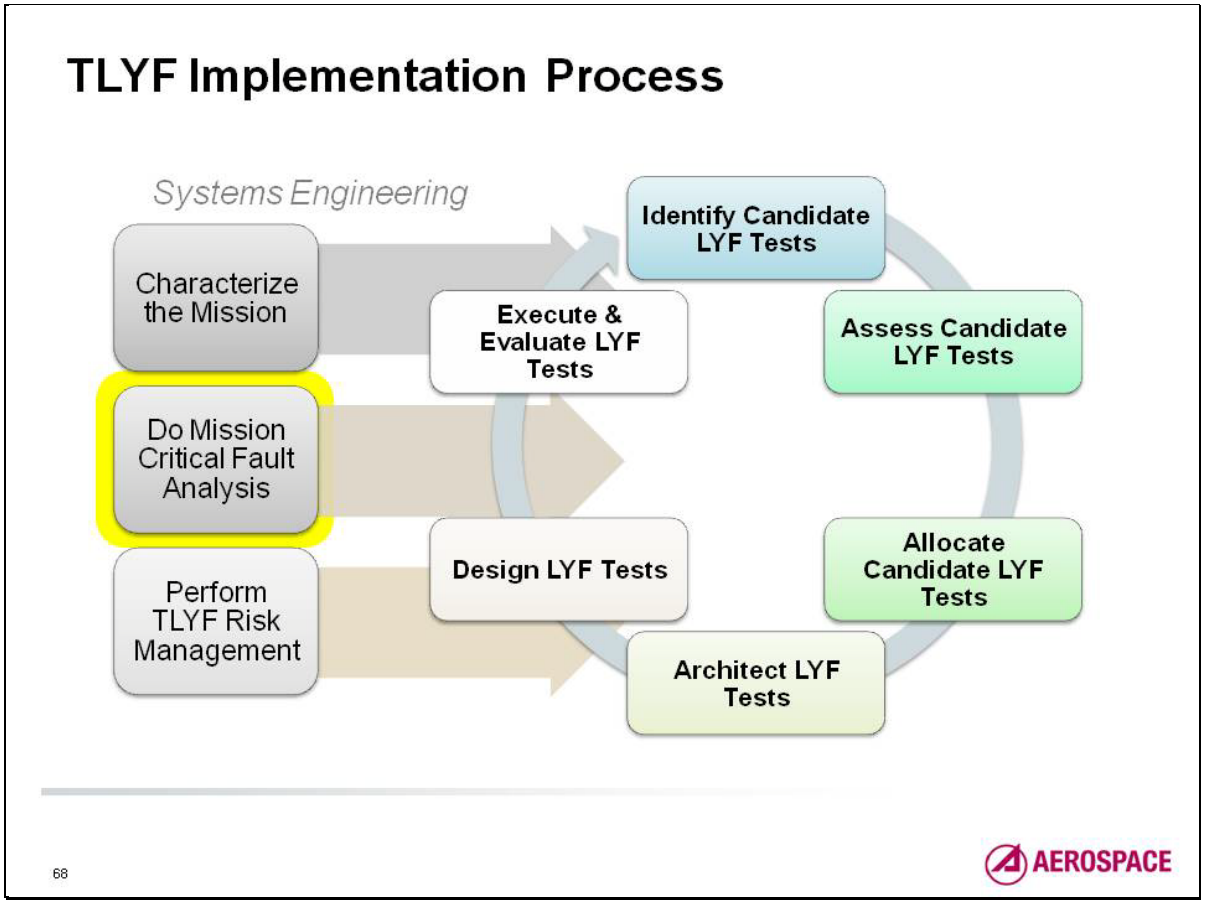
- It is the appropriate level which reflects the mission level situation and functional relationships
- It is the highest testable level
- It is useful to be done at a lower level for additional perceptivity
  - *Results feed into higher level testing*
- It is necessary or useful to be done at a lower level for risk reduction
  - *Find and fix flaws earlier*

67

AEROSPACE

One LYF risk reduction approach that has been used successfully by some organizations is to integrate the space and ground segments very early in development, and use the ground system as the EGSE during SV integration and test. Although both SV and ground system have only partial functionality when the integration initially occurs, this approach provides an early validation that the ground system can command the vehicle and process telemetry. Particular threads and scenarios can be executed as the integration permits. This process enables discrepancies to be discovered and fixed much earlier than is the case in the more traditional development process.

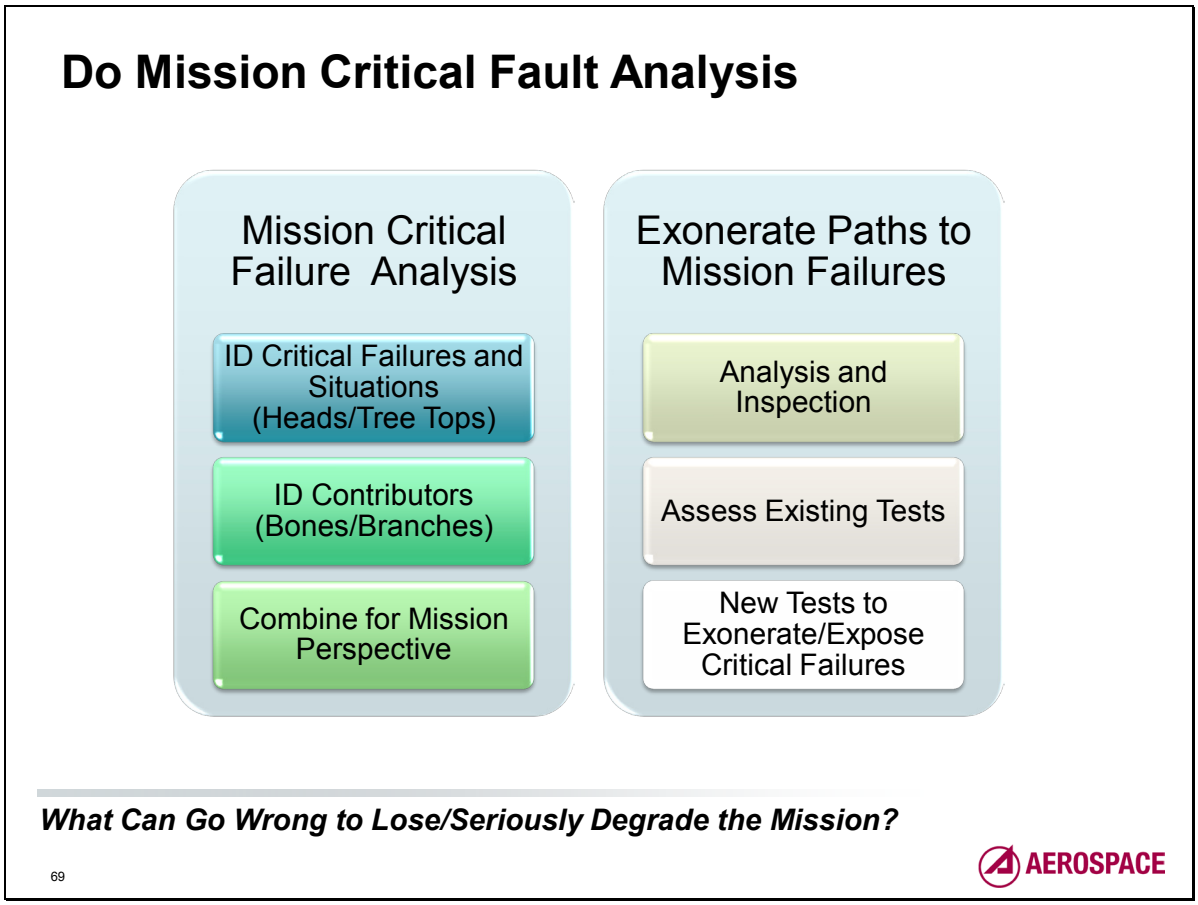
Slide 68




Fault analysis is a technique typically used as part of a failure investigation. In a failure situation, the actual failure indication is known, e.g., no communication from the space vehicle. A team of experienced investigators of various specialties, generally independent of the project, is gathered for a limited period of time and presented with design and flight data. They proceed to identify a number of possible contributors to the observable failure. Project personnel then gather further evidence to exonerate or to implicate those possibilities.

When critical fault analysis is performed pro-actively, before a failure occurs, it provides, among other things, an excellent platform and priority for LYF tests. And thus, it is injected into the TLYF process.

Slide 69




Most programs require a "failure modes, effects, and criticality assessment" (FMECA, or FMEA) as part of the design process. This is a valuable design assessment technique that systematically steps through hardware designs looking for downstream effects of component or part failure, particularly single point failures. The shortfalls of FMECA from a system design assessment perspective include (1) it does not take software into account, and (2) it does not address mismatches – of timing or transactions – that can cause a system to not perform as intended, but not be recognized as a hard failure.

With a TLYF perspective, key questions are expanded to include: (1) what does/can mission failure look like for this system, and (2) what can contribute to such failure(s)? The answers to those questions are derived from a different approach to failure assessments, based on fault-tree or fishbone analyses. These serve to quickly focus on the most critical kinds of failures for the system being developed, and to include a broader representation of failure contributors. Once such fault-tree or fishbone diagrams are defined, it can be determined what kind of evaluation is necessary to exonerate a branch or bone (flaw), and thus lower the risk of the failure condition occurring.

The result of the first four steps of the TLYF Implementation process is a list of potential LYF tests, which may be longer or more difficult to achieve than the program resources can support. The Mission Critical Fault Analysis can be used to prioritize the list of potential LYF tests on the basis of which are more likely to reveal mission-critical flaws. The technique also serves as a basis for using certain tests or other evaluation techniques for their flaw detection/exoneration abilities, independent of their use for requirements verification. Where exoneration depends on a "like you fly" test, new

candidate LYF tests must be added to the assessment list. This technique can also point to the incorporation of specific flight characteristics into a “non-like you fly” test.

Slide 70

# Identify and Handle Mission Critical Failures

- Description:
  - *Step can be accomplished as part of the systems engineering process outside the TLYF process. However, the results are needed to ensure the maximum efficiency of LYF testing in perceiving mission critical failures.*
  - *Identify set of mission critical failures and mission critical situations*
  - *For each mission failure, identify potential contributors to the failure*
  - *Each potential contributor needs to be exonerated or handled*
  - *Because of the complexity of this step, each of the sub-steps will be discussed separately.*
- When used:
  - *Initially for PDR*
  - *Updated at CDR*
  - *Updated after design changes*

***Apply the TLYF Lens***

70

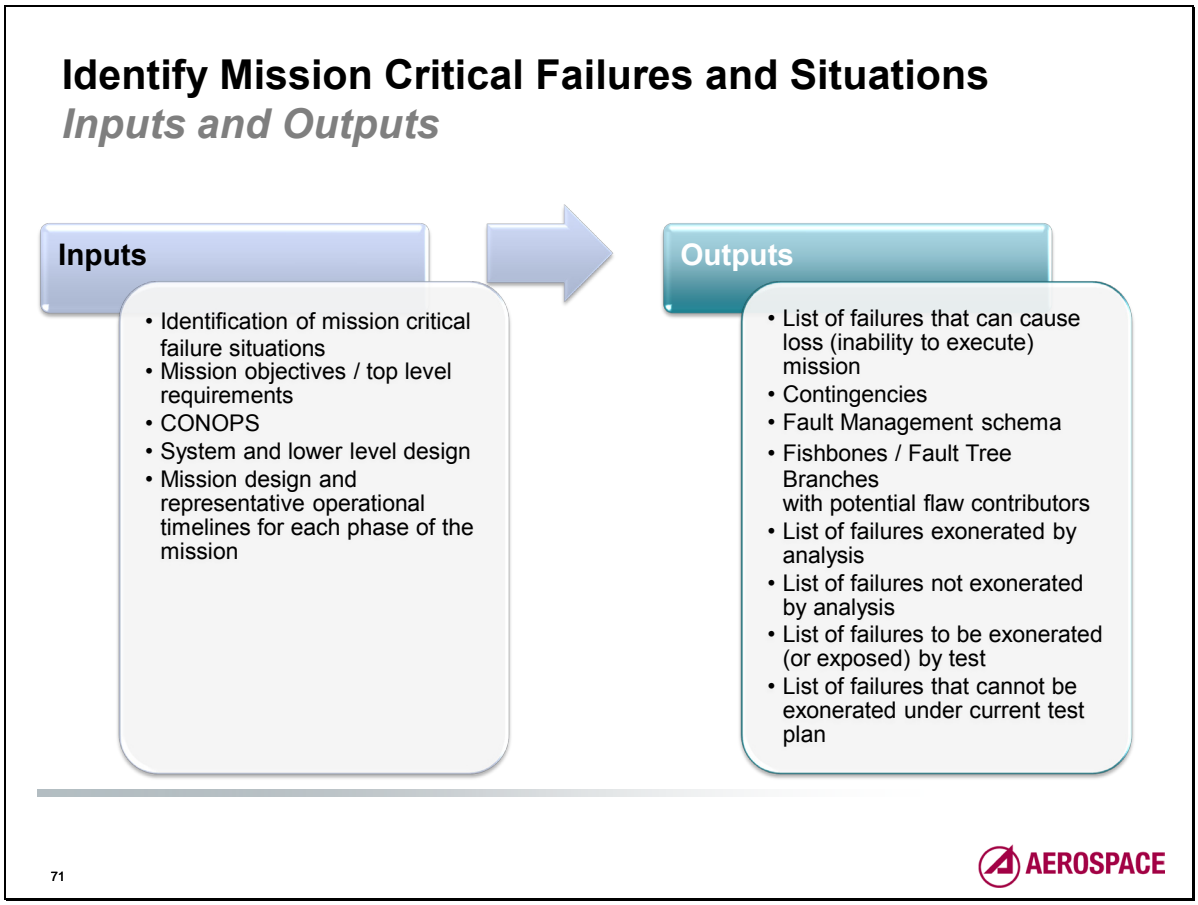
AEROSPACE

Because this step is looking at mission failure, it is important to include all segments of the system, not just the SV.

Defining what constitutes mission critical failure situations can be accomplished after the initial development of the CONOPS. There must be at least a preliminary design in place to perform this step in detail. Performing the Mission Critical Fault Analysis prior to PDR may expose some weaknesses in the design that can be addressed through design. It will also refine the LYF tests at an appropriate time in the development.

The requirement for this type of assessment should be included as part of Pre-Systems Acquisition phase strategy decisions. Programmatic resource decisions regarding the execution, abridgement or deletion of such tests must be made with the understanding of the risk, and the possible effects of not finding flaws that could contribute to mission failure.

Slide 71




The mission critical failure situations ("fish heads"/"tree tops") can begin to be identified as soon as the mission objectives and top level requirements are in place. The CONOPS, mission design, system design, lower level design, and operations timelines are likely to suggest similar additional failure situations.

The results of performing a mission critical fault analysis will be several lists: critical failure situations, failure paths, allocation of exoneration to analysis or test, and potential contingencies for later development. The fault analysis at the level of space vehicle design will provide the basis for on-board fault management.

Slide 72

## Mission Critical Failures and Mission Critical Situations

- **Mission Critical Failure** – an on-orbit condition that meets one or more of the following criteria:
  - *Mission ending failure, i.e., payload or spacecraft bus is no longer capable of supporting the mission objectives*
  - *Degrading conditions whose trend indicates a loss of mission before Mean Mission Duration (MMD) or design life*
  - *Repetitive transient conditions that, uncorrected, would lead to an unacceptable loss of mission performance, data or services*
  - *Condition that causes inability to meet minimum performance specifications*
- **Mission Critical Situation** – A set of conditions where nothing has failed, but the mission cannot proceed
  - *Example: Satellite with processor susceptibility to single event upsets in orbit with mean time to upset much less than mean time to recovery from upset.*

72

AEROSPACE

When doing mission critical fault analysis, it's important to assess both "Mission Critical Failures" and "Mission Critical Situations."

Mission Critical Failures are primarily related to a "hard" system failure or degradation serious enough to predict a time or condition when some fundamental mission capability will be lost. Mission Critical Situations do not necessarily highlight a specific system failure or degradation trend, but are an operational inability to execute a mission.

Slide 73

# Key Definitions

- **Contributors to fault –** any single flaw or combination of conditions that directly leads to the fault condition.
- **Flaw –** Defect, anomaly, hard failure, soft failure, interaction mismatch, or any other condition that causes a detectable problem in the system.
- **Exonerate path to fault –** produce evidence to show that the potential flaw is not present under flight conditions.
- **Autonomy and Fault Management –** Software, hardware, or combination that detects specified fault conditions and automatically (without human intervention) executes pre-defined logic that either allows direct recovery or entry into a safe mode.
- **Contingency –** Procedure written to allow ground controllers to detect, assess, and recover from selected fault conditions.

# What Does Mission Failure Look Like?

- Could happen to most vehicles/ systems (contingencies)
  - *No communications signal from vehicle*
  - *Failure to respond to commands*
  - *Insufficient power to support mission*
  - *Others?*
- Electro-optical sensing mission
  - *No sensor data*
  - *Poor quality sensor data*
  - *Others?*
- Communications mission
  - *No signal evident on user equipment*
  - *Significant signal dropouts*
  - *Others?*
- Navigation mission
  - *Constellation gap*
  - *Others?*

74

AEROSPACE

Slide 75

## Lessons from Mars Polar Lander:
### *Test What You Fly (Post Repair)*

- Faulty touch down sensor logic caused vehicle to crash
- A LYF test had been run, a hardware problem was detected and repaired
  - *That test was <u>not</u> rerun after the repair*
  - *Original problem masked the second problem (hardware/software interaction)*
- **Lesson**: Test What You Fly
  - *A repaired item is a different entity than the pre-repair item*
- **Lesson**: Test How You Fly
  - *Test across mode and phase transitions*
  - *Be aware of range of initial conditions for flight situation*

Mars Polar Lander

*Courtesy NASA/JPL-Caltech*

***Loss of Mission***

75

AEROSPACE

The NASA Mars program suffered back-to-back mission failures in 1999. The TLYF lessons learned for three NASA programs will be discussed.

First, the Mars Polar Lander crashed on the Martian surface. Its onboard HW and SW logic was supposed to sense touchdown and immediately shut down the descent engines. The failure investigation showed this logic was faulty and it had never been tested in the flight configuration at the SV level, due to a decision not to retest after a repair.

Late repairs tend to have less rigorous review and control of procedures. Ad hoc repairs are a frequent source of additional problems. Inadequate or no post-rework test of the repaired item is considered a "Test What You Fly" (TWYF) violation.

Slide 76

## Lessons from Mars Climate Orbiter:

### *Design LYF Tests for Ground/Space Interactions*

- English to metric units mismatch error
  - *Metric units were required for flight equipment*
  - *English units were used in ground software tool, apparently in violation of requirement*
  - *Ground software was deemed "non-critical" and so not tested with flight software*
- **Lesson**: Conduct "total operations chain" test to find ground/flight interaction problems
- **Lesson**: Anything that touches/ interacts with critical flight equipment and processes is itself, by definition, "critical"


*Courtesy NASA/JPL-Caltech*

***Loss of Mission***

76

AEROSPACE

The Mars Climate Orbiter was the second failure for the Mars program.

The loss of Mars Climate Orbiter is a classic case of misunderstanding the criticality of ground planning tools. The SV impacted the surface of Mars rather than entering its orbit due to improper thruster commanding for mid-course trajectory corrections. The SV expected commands based on metric calculations, but one mission planning tool, whose software was deemed "not critical" used English units. This is an example both of not using all tools in a total operations chain fashion, and of not performing a fault-tree/fishbone analysis for mission critical situations during the design phase.

As another example, wiring between an SV and its LV was faulty. The SV never separated, resulting in loss of mission. Investigation showed that the interface was checked with improperly configured ground SW. The proper SW load would have identified the problem. This is an example of violating the "test what you fly" aspect.

Slide 77

## Lesson From Mars Odyssey:
## *Do a Mission Critical Fault Analysis During Design Phase*

- Mars Odyssey, the next Mars mission to follow the two Mars failures in 1999, pioneered a method of holding the "failure review board" prior to launch
  - *This technique has been used on subsequent planetary projects*
- Method puts the focus on identifying flaws that can kill or severely wound the mission
- Use those revelations to focus the test program to validate or exonerate the existence of those flaws
- **Lesson**: Integrate critical flaw analysis into TLYF process
  - *Do the "Mission Failure" Investigation Pre-Launch*


*Courtesy NASA/JPL-Caltech*

***Successful Mission!***

77

AEROSPACE

The program and mission management for the next project in line, Mars Odyssey, observed that the failure review teams were remarkably efficient at identifying a number of serious flaws, in both developments, that had escaped the normal design review, verification, and readiness review processes.

They proposed that something like a failure review board, performed by people already involved with Mars Odyssey, be convened to hypothesize mission failures and identify possible contributors to those failures. Using a fault tree analysis approach, they were able to identify a number of potential problems. These were investigated and mitigated as necessary. We conclude that "failure reviews" are most effective if performed pre-flight. Other Mars projects have continued to use this technique as part of their design process.

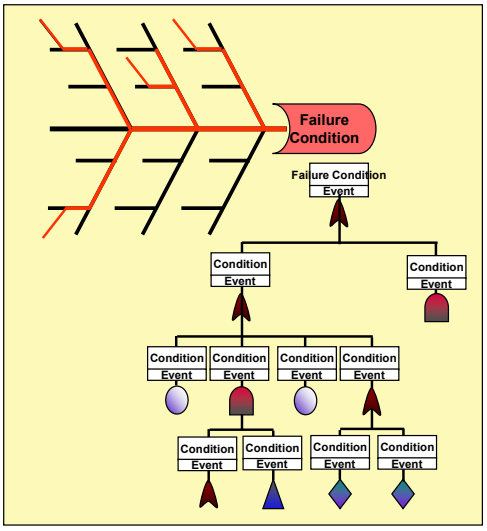
This serves to focus the development team on what can go seriously wrong and adjust designs, manufacturing processes, and verification techniques to ensure that critical flaws are not introduced, or to catch them before they escape to the mission.

Implemented as part of project development, there are key differences from the post-failure investigation. While in the design phase a much larger number of potential mission critical failures or situations will need to be examined rather than would be examined after an actual failure. Instead of gathering an independent team, it may be more efficient to use project people already familiar with the mission and its implementation.

Slide 78

## The Hunt for Red Flaws

- Fault analysis (FA) optimally should be done in the preliminary design phase
  - *FA is the other end (top down) of the Failure Modes and Effects Criticality Assessment (bottoms up)*
  - *FA is a directed analysis of various levels of design to further understand flaw scenarios (known unknowns)*
  - *Problems identified in this phase can possibly be mitigated by design changes*
- Determine what failure looks like to your mission
  - *Non-recoverable*
  - *Mission specific*




***Benefit: A rigorous event/fault tree can be used as a basis for other activities (automated fault management, contingency planning)***

78

AEROSPACE

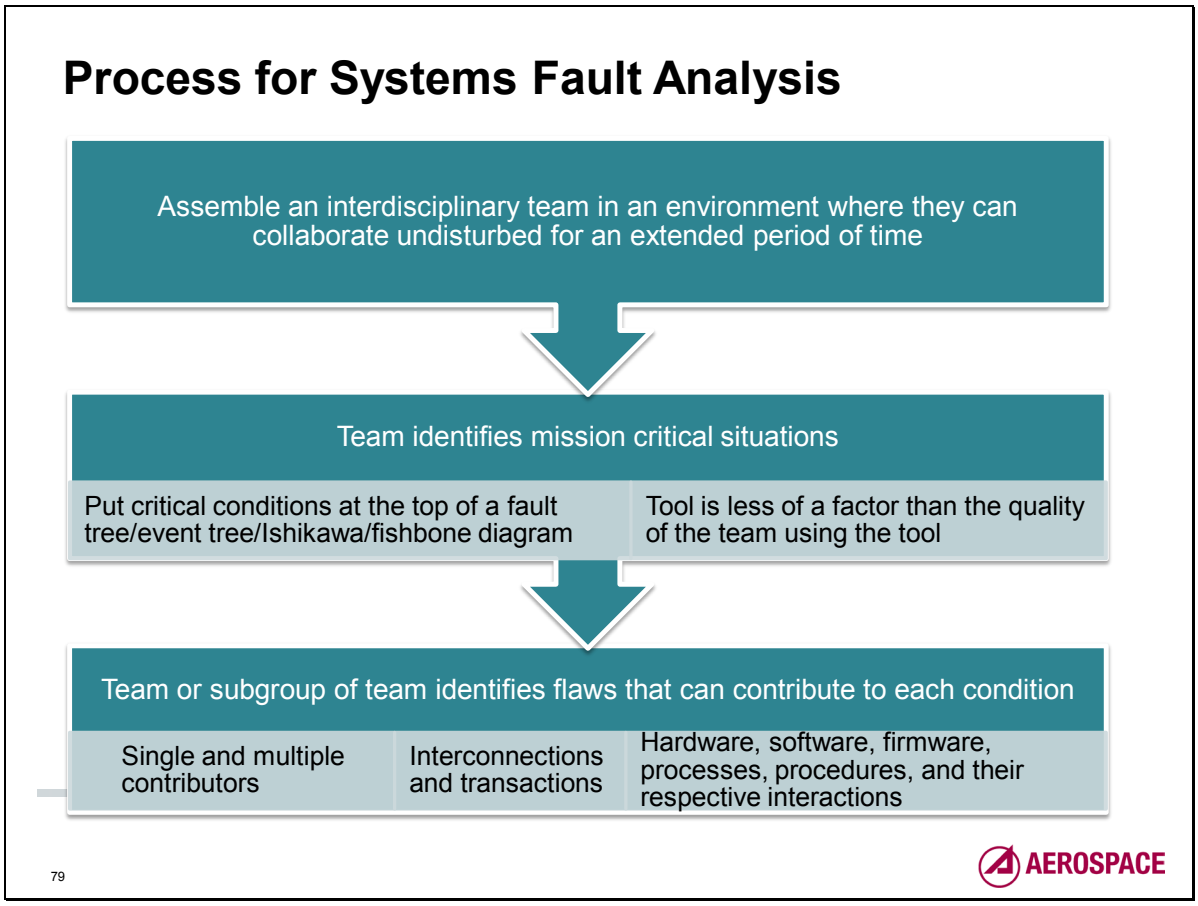
Several useful tools and techniques already exist to focus design, test, and risk processes on the most critical aspects of a mission. These include, but aren't limited to, fault tree analysis, event tree analysis, and Ishikawa diagrams.

The most important "tool" is to get a critical mass of diverse experts into a room for a few days uninterrupted by phones or program distractions. Whatever failure analysis technique the group is comfortable with will be the best one for this process.

This technique is complementary to the frequently used failure modes, effects, and criticality analysis (FMECA or FMEA). Where the FMECA is primarily driven by hardware schematics, the fault analysis allows a mix of hardware, software, process, procedure, and human contributions to a failure.

The connection of this technique with TLYF is twofold: a focus on potential flaws, and a prioritization scheme for TLYF exceptions analysis. TLYF is a test technique perceptive to mission operability and integration/end-to-end flaws, so it helps to develop a "what can go wrong" mindset when doing designs, manufacturing, and verification. A complex space system with large software elements will have a large number of latent flaws and an almost infinite number of potential flaws. However, only some of the latent and potential flaws will contribute to, or cause, mission critical situations when the right combination of attributes are present.

Slide 79




The Critical Fault Analysis process can be summarized as follows:

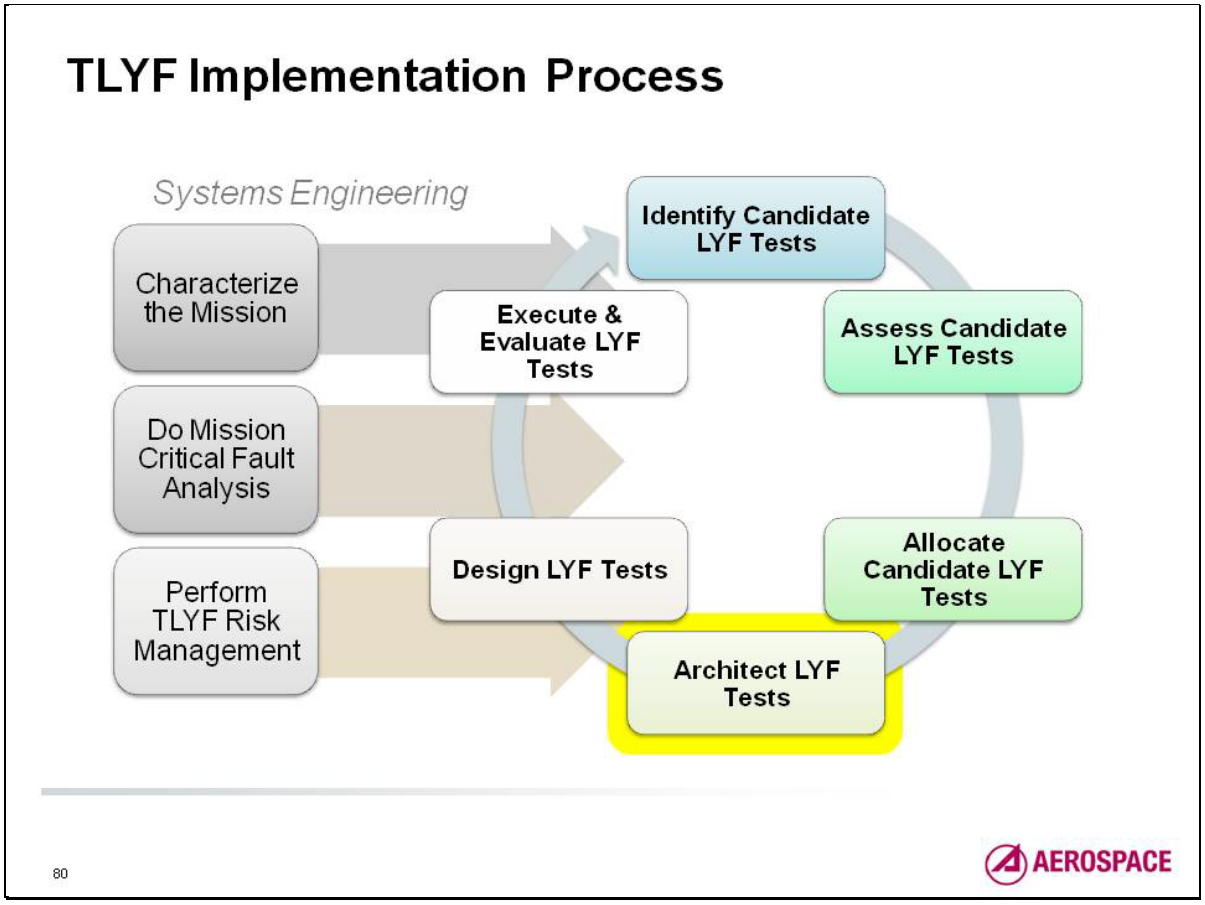
- Identify mission critical situations.
- Do the "failure review board" pre-flight.
- Use one or more logic tools or techniques to identify possible contributors to each mission critical situation.
- Identify methods for verifying the existence or exonerating the absence of each contributor.

This is a system engineering technique that can and should be used for more than the TLYF assessment process. So how does it specifically apply to TLYF? Another set of steps must be followed:

- For those contributors that need to (or would best) be verified or exonerated by a test, determine whether or not the test needs to be "Like You Fly" to be certain of the exoneration or existence of the flaw.
- For each test that must be "Like You Fly," determine which mission characteristics must be included as part of the test.

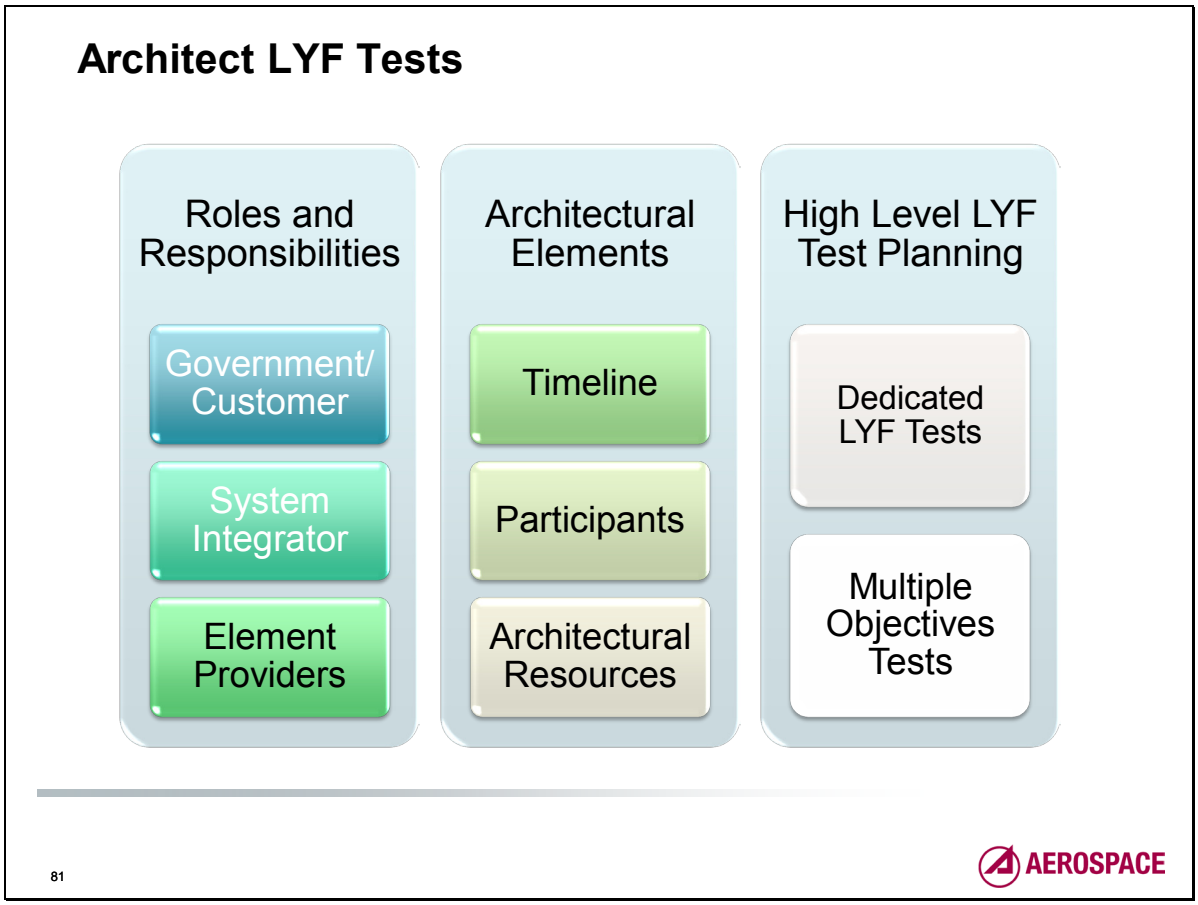
- Any characteristic that cannot be adequately incorporated into a LYF test is deemed a mission critical TLYF exception. These are the exceptions that then need to be identified as risks, and mitigated and monitored accordingly, as an input to a program's risk management process.

Slide 80




This step takes each accepted LYF test and begins the process of turning it into an executable test within the framework of program resources.

Slide 81




This step includes all the traditional architectural elements as identified on chart 33. All of these elements can be applied at every level of LYF testing. Architectural decisions for a LYF test may be dependent on whether it is a standalone test or is being developed in concert with a test that will address several objectives, only one of which is to validate mission operability.

Slide 82

# Architect LYF Tests

- Description:
  - *Assign roles and responsibilities to involved organizations to create a high level test plan for the flow of LYF tests involving all the participating elements.*
  - *Create a high level test plan for each LYF test.*
    - Review the program's test plans and identify tests in which LYF test objectives can be combined with other tests with different objectives.
- When used:
  - *During project planning phase to drive contract requirements*
  - *In conjunction with PDR*
  - *Update at CDR and later as needed*

82

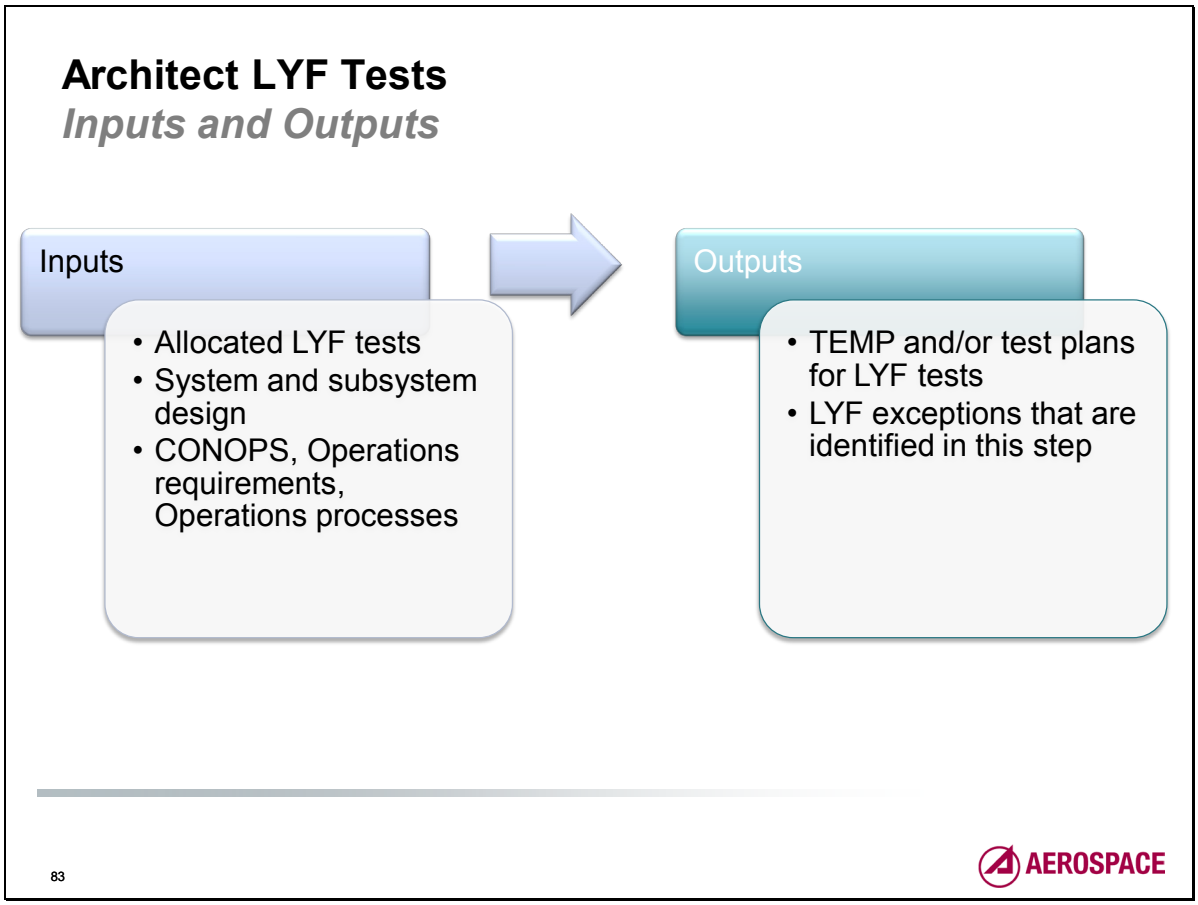
AEROSPACE

During project planning, the program office needs to consider the roles and responsibilities of the participants in the test, particularly at a high level. One of the decisions that the program office will need to make is which organization is responsible for architecting the tests as the program proceeds. As described on a later slide, the architect must make key decisions as to the allocation of resources for LYF tests. This responsibility can be retained by the program office, or levied onto the system integrating contractor.

An important component of this step is identifying opportunities to fit the LYF tests into the development and testing process. This is the key to a cost-effective approach to LYF testing. As mentioned before, by developing the ground system incrementally in parallel with the SV and using the developing ground system as SV EGSE during SV integration, many LYF issues between the SV and ground system will be revealed early in the development process.

Similarly, it may be possible to add LYF tests to the testing done during environmental testing in the TVAC chamber. However, this may require augmenting the TVAC configuration. For instance, a LYF normal operations test in TVAC would need to include a communication path to the ground system. If TVAC environmental testing is done before the flight or ground software is mature (a Test What You Fly violation), the program may consider moving TVAC on the schedule or may need to schedule a second use of the TVAC chamber when the system is mature.

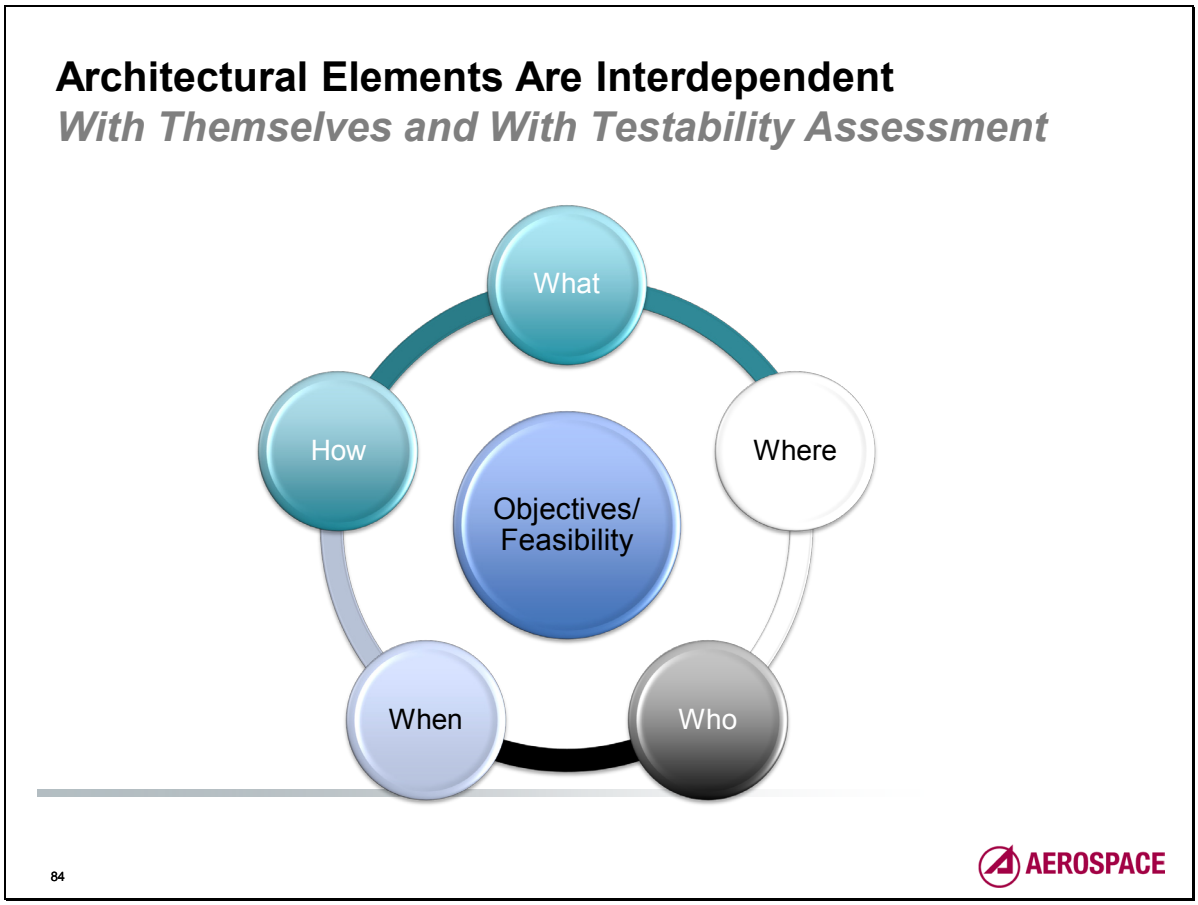
Slide 83




By the completion of this step, the LYF tests are defined enough to be documented in the TEMP (or equivalent) and in initial test plans. They should also be incorporated into the Integrated Schedule, and should be deconflicted with other events.

This process may lead to new LYF exceptions for each test; these will need to be evaluated for criticality.

Slide 84




The architectural elements are interdependent and the following elements must be considered prior to architecting a LYF test for products and assets (i.e., ground, space, user). Test resources (i.e., test beds, simulators, stimulators) and participants are included in architectural elements.

- **Who** should participate?
- **What** should be used in the test?
- **Where** should each "what" reside? (i.e., factory, development setting, special test facility)
- **When** must each "item" be available? (i.e., resource availability, program schedules)
- **How** to make it happen? (Connectivity and interdependence of tests in overall test flow, logistics)

By addressing these key questions comprehensively, the LYF architect can determine TLYF objectives and feasibility.

Slide 85

## Role of the Architect

- The role of LYF test architect is to be the primary decision authority for structure of the test
  - *Architectural decisions are tied to acquisition*
- The primary LYF test architect should:
  - *Identify trade-offs between the test objectives, the architectural elements, and feasibility/perceptivity*
  - *Choose an optimum set of architectural elements from the alternatives*
    - Architect must be able to make priority, resource, and risk decisions concerning what will be included and excluded from the LYF tests
  - *Document architectural decisions in an appropriate level of test documentation to bound LYF test design*

85

AEROSPACE

The plans produced by the architect must be executable within program constraints and must meet the objectives of LYF mission validation. The plans must provide sufficient definition to direct the test designer who, in general, will have a more limited systems perspective, in developing the detailed test plans.

Slide 86

## Responsibilities of the Architect

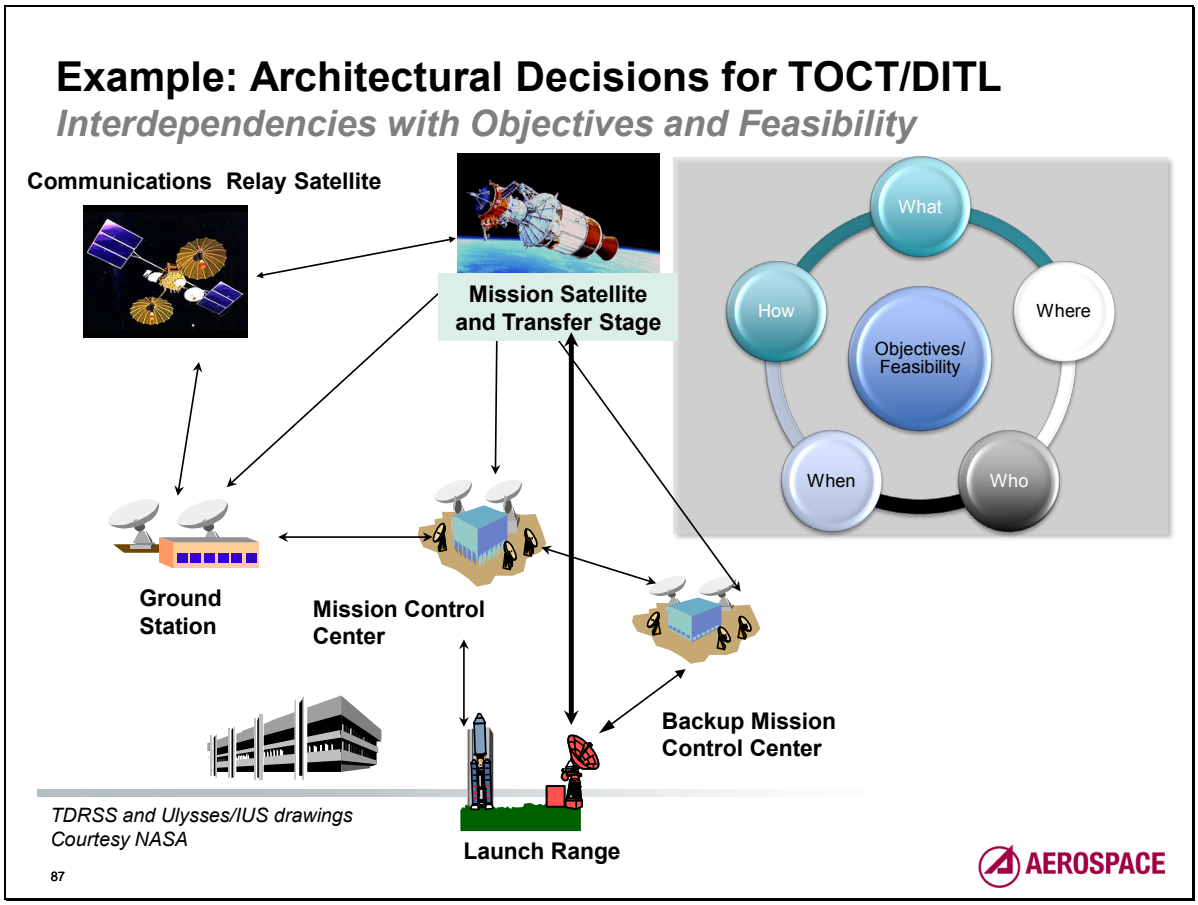
- Specify the test objectives
- Establish test entrance and exit criteria
- Determine the scope
  - *Test coverage of applicable mission phases and capabilities*
- Identify the elements, organizations and participants involved, e.g.:
  - *Ground command and control*
  - *Mission operations*
  - *Mission planning*
- Identify test roles and responsibilities of involved organizations
- Identify the test and mission processes
- Identify the assets needed, e.g.:
  - *Mission hardware/software*
  - *Stimulators*
  - *Simulators*
  - *Special test equipment*
  - *Facilities*
- Identify the applicable mission characteristics for each test
- Identify the level of equipment and software readiness needed for test
- Identify the level of fidelity needed for stimulators, emulators, simulators

86

AEROSPACE

This chart is a checklist of the elements that must be defined by the architect. It is important that the architect, in defining these elements, ensures that the test will be executable within the schedule and resource constraints of the program. This is especially important in determining needed levels of readiness for hardware, software, procedures and personnel, and in determining fidelity of stimulators, emulators, and simulators.

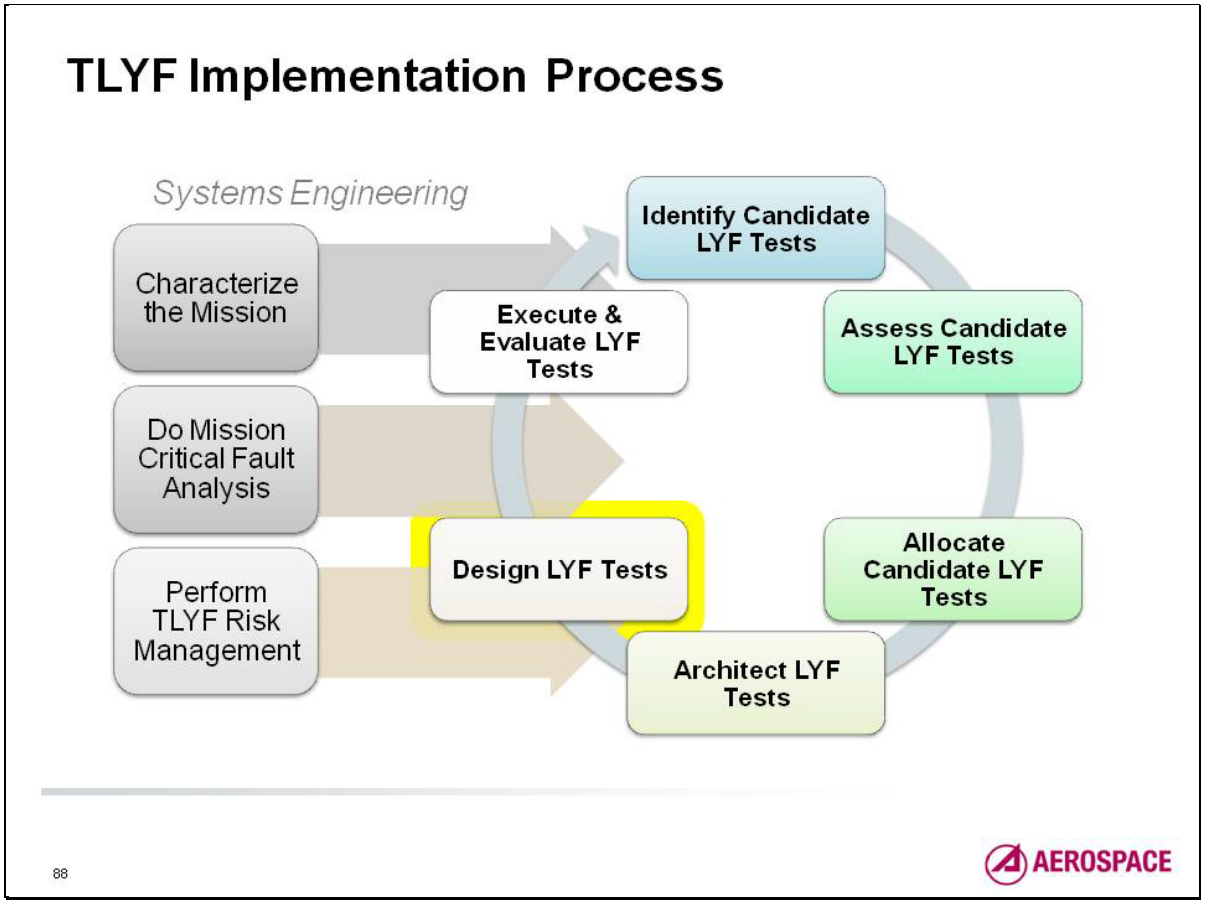
Slide 87




This notional diagram includes examples of elements for each segment, but the diagram is not to imply any specific physical implementation. It could be the case that a particular set of requirements are best served with a distributed set of elements, while another might have some elements co-located.

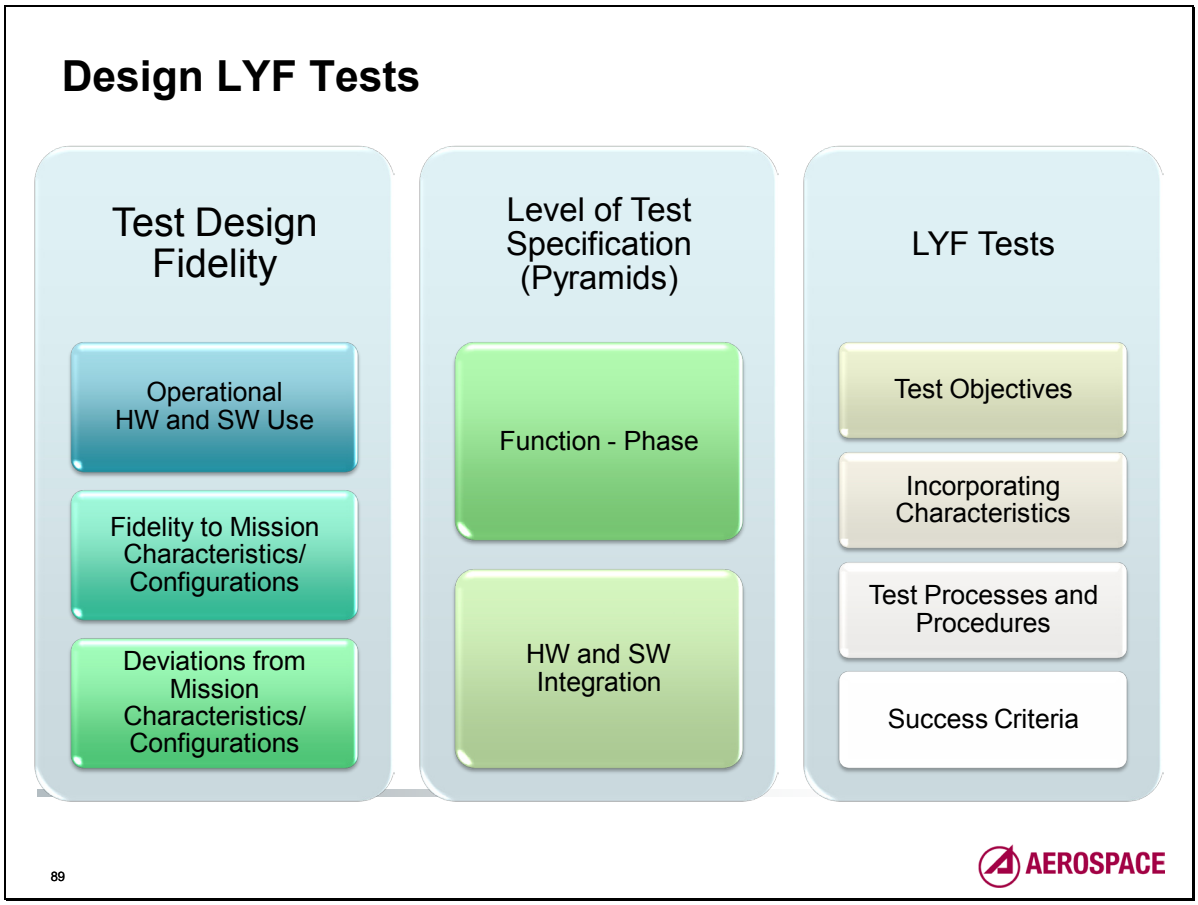
| | |
|---|---|
| Space Segment | Mission Satellites, COMM Relay Satellites |
| Ground Segment | Ground Stations, Mission Control Center (MCC), External C&C Center |
| User Segment | User Terminal, User Elements (e.g., data processing center) |
| Launch Segment | Launch Range and related facilities |
| C&C | Command and Control |

Slide 88




This step takes an architected test through the test design elements, considerations, trade-offs and challenges.

Slide 89




LYF test design must first deal with decisions associated with the fidelity of the test characteristics and processes compared to the mission characteristics and processes. Some aspects of fidelity may have been dictated or constrained in earlier steps. The remaining aspects must be dealt with in this step. Similarly, some decisions as to where high level tests should allocated to each of the test pyramids have already been made, but there will be more detailed decisions that will need to be made about what levels of functionality and integration are needed from a test design perspective.

All tests, not just LYF tests, must have specific objectives defined. LYF test design must address the particular ways that mission characteristics will be incorporated into the test; the extent to which mission processes and procedures will be used to execute the test; the way in which test processes, equipment, and procedures must be used to either emulate the mission or provide for the safety of the items under test. Some high level test success criteria may have been provided as an input to this step, but lower level success criteria will need to be determined by the test designer to provide a decision tool to allow steps of the test to progress.

Slide 90

## Design LYF Tests

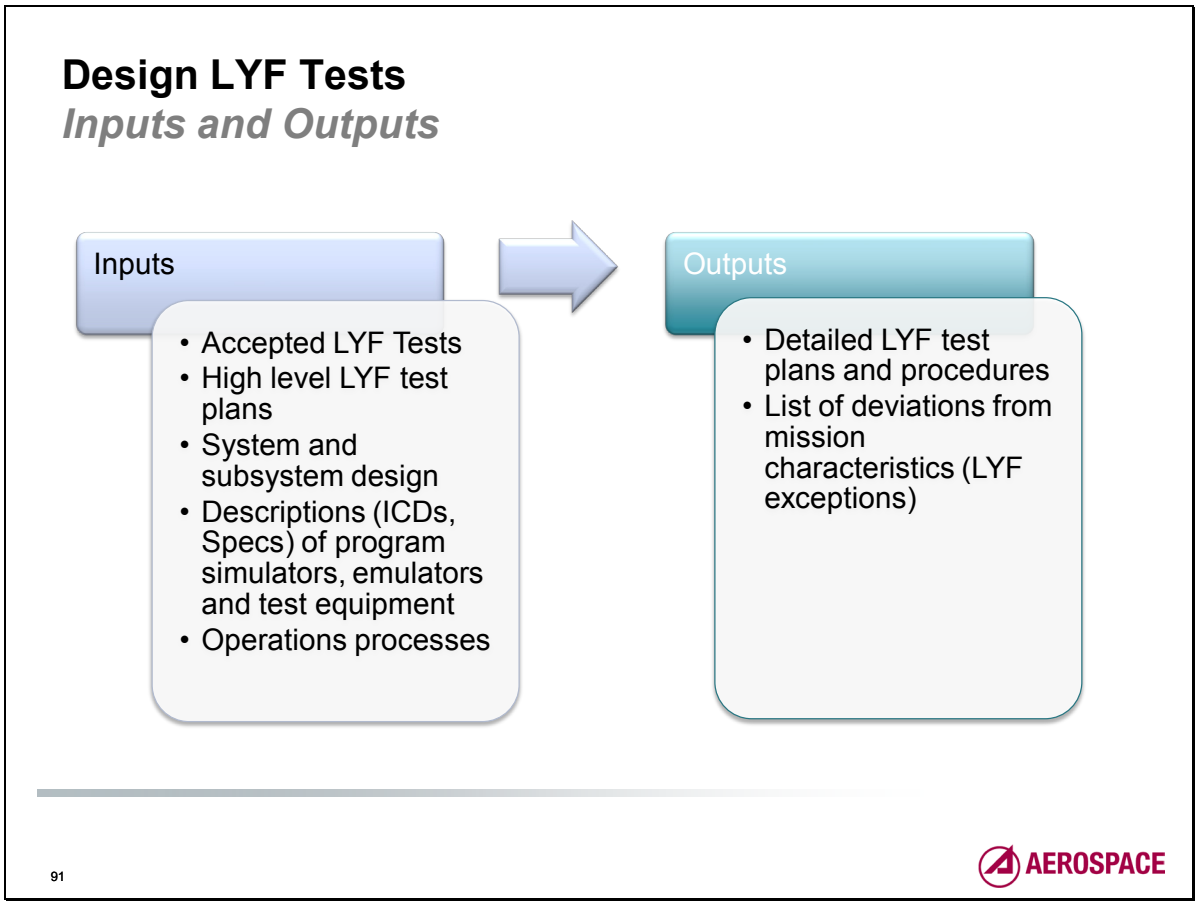
- Description:
  - *Apply basic principles and elements of test design which includes well defined goals, the test conditions, type of testing, and level of testing (application to the pyramids)*
  - *Create detailed test plans that meet the identified test objectives and success criteria, incorporating mission characteristics and configurations as appropriate for mission emulation and good test design principles.*
- When used:
  - *During system design*
  - *For PDR – initial draft*
  - *For CDR – final*
  - *As an iteration from Critical Fault Risk Feedback (after CDR and prior to Production)*





All basic principles of good test design apply to the design of LYF tests. The basic progress of test design through the development phase is the same as for other tests. One thing that is unique to LYF test design is the iterative process with critical fault analysis and the need to understand design decisions in terms of what flaws may be missed as a result of those test design decisions.

Slide 91




Each accepted LYF test will need to be designed. That design will be constrained by the developed test plans. The LYF test design will be constrained or enhanced by design decisions relating to simulators, stimulators, emulators, test beds, and other test equipment. The design process for a LYF test may, in turn, influence the designs of those items. The test design will need to account for system and lower level design considerations and constraints that affect the lower level details of the operational usage of the items under test. The process of designing and executing a LYF test will, in turn, expand the understanding of how the item or system must be operated to account for the as-built equipment and software, rather than the as-designed items.

As with any test design process, the end result is a set of test products, including detailed test plans and test procedures. The LYF test process includes a product that is not generated by the design process for other tests: the LYF exceptions. This is a detailed accounting of the deviations between the applicable mission characteristics and the test characteristics.

How to handle the exceptions will be explained in the last step of the TLYF process.

Slide 92

## Test Design Required Elements (1)

- Test objectives
  - *Mission critical events/timelines*
  - *Associated characteristics*
- Test cases (nominal, off-nominal and stress) and rationale
  - *How are things expected to happen?*
  - *Is there more than one way for "nominal" to occur?*
- **Initial, transition, and end** conditions for the test, or each section of the test

***Note key deviations from mission inputs***

92

AEROSPACE

Test objectives for a LYF test must relate to mission activities and characteristics. These are what distinguish a LYF test from other types of tests. The most important objective is to validate that the mission critical activities included in the test can be successfully accomplished in the context (mission characteristics) of how they will be executed during the mission.

Mission characteristics include, but are not limited to, those associated with orbital parameters, external and internal environments, flight operations, mission objectives, mission concepts of operations, and hardware and software configuration. Examples of mission characteristics include: (1) orbit period, (2) eclipse duration, (3) radiation environment, (4) atomic oxygen environment, (4) visibility to communication and control assets, (5) network operation processes and cycles, (6) mission phases and modes, (7) mission tasking, (8) mission planning, (9) command planning, (10) absolute time, (11) clock consideration, (12) duty cycle, (13) timelines, (14) activity duration, (15) activity sequences, (16) activity constraints and considerations, (17) signal services, and (18) data product creation and dissemination.

The test designer must consider which test cases to include. For LYF tests, the organization of the mission will influence the identification of test cases, as in the division of the mission into phases. The design of the system will influence the inclusion of other test cases, as in the interactions between elements. When thinking about days-in-the-life tests, it is necessary to identify how many different kinds of days and cycles there are. A mission that has a weekly planning cycle, a daily planning cycle, and a priority path for special operations that needs to be incorporated outside of normal planning processes may give rise to a number of test cases. A part or subassembly that may be used in different circuits with different power levels, duty cycles, and orbits may need a number of test cases to show

suitability for a variety of applications. Test cases should also include those that specifically include fault and contingency conditions. Fault or contingencies that lead to the usage of backup or redundant items may be the basis for including “nominal” test cases that use those backup/redundant items.

Some mission activities may have a highly constrained set of initial conditions and few, or no, defined alterative execution paths. Those will be the ones with few possible test cases, and it may be feasible to do them all. Other mission activities will have a relatively wide set of options for initial conditions and execution paths. These will need more test cases, especially if fault conditions could result in even more execution paths. A timeline test of the ascent mission phase usually has a fairly constrained initial condition, and an obvious test case is to run the system from the initial condition (T+0 or some pre-launch known configuration point) through satellite separation or the collision avoidance maneuver. For systems that have fault management active in this phase, it would be prudent to include some fault cases. One obvious case is the failure from a primary to backup computation item to ensure that the mission can succeed in the case of redundancy selection. Software specifications have long included the recommendation for including stress cases. In the case of a LYF test, the stress may come from other sources than the use of the software. System tests that include ground systems should include test cases that stress the processes and personnel running the various elements of the ground system.

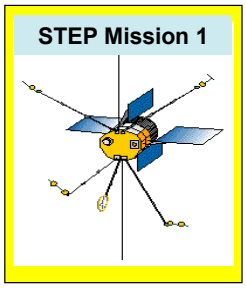
The reason to include transition conditions as a test case factor is to avoid the premature conclusion that separate mission phases or activities are independent and have no influence on the phases or activities that follow them. A test case that induces a transition to a safe mode may also need to include a recovery from safe mode to ensure no flaws exist in either transition.

Slide 93

## Lesson from STEP Mission 1

### *Test Design as Function of Test Objectives*

- Mission timeline is driven by the clock
  - *Time flows in one direction*
- Clock handling during test was not like flight
  - *Consequences of resetting to "zero" time*





T = 0, ~100 minutes @ perigee

- STEP M1, with one primary payload and 5 secondaries, was to fly a LEO elliptical orbit with a period of about 100 minutes
- Contractor performed "Design Reference Timeline" scenario of single orbit (100 minutes) operations during System TVAC
  - *Clock was reset to "0" at every "perigee" and command sequence for orbit repeated*
  - *Deviations from mission were not identified and evaluated*
- Later in the test flow a LYF test objective was added resulting in a 12-hour "Day in the Life" test in ambient
  - *~ 15 minutes into 2nd orbit, secondary data overwrote primary data buffer*
- **Lesson**: LYF test objectives must be reflected in the test design

**Diving Catch: Loss of Primary Mission Data**

93

AEROSPACE

An example from the test program of the Space Test Experiments Platform (STEP) Mission 1 project illustrates how differently test objectives influence the test results. A one-orbit "design reference timeline" scenario had been created early in the design phase for all designers to use as a basis for time/orbit based design considerations. Traditional test design seeks to hold all but one independent variable constant, so that the effects of changing one (independent) variable can clearly be observed. One primary objective of the system level thermal vacuum test (SVTV) is to identify vehicle behavior that changes as a function of temperature. To achieve that objective it is necessary to run the same functional tests, including the reference orbit timeline, at different temperatures. At the time, the contractor identified the design reference orbit as a "like you fly" aspect of their SVTV test.

But while this is a necessary objective and a valid approach to the SVTV objective noted above, it is different from the objective to find critical flaws in the operation of the SV as it will be run during mission operations. This second objective requires a longer timeline to probe accumulation, timing errors, and other problems associated with a more complete set of mission activities. One key activity not included in the reference orbit was the inclusion of mission equivalent ground commanding and data retrieval. This program had already done a "factory compatibility" (compat) test demonstrating that sample "no-op" commands of each type could be sent by the ground station and properly received by the vehicle. The compat test also demonstrated that the vehicle could send representative telemetry of each type and have that properly interpreted by the ground system. There was also the assumption that performing the reference timeline in SCTV completes the operations activity, even though it does not involve interactive commanding and payload telemetry with the ground station. Even though this was a "Class C" development, the lack of evidence that the system could

consistently provide useful primary payload data, was compelling enough for the program management to authorize a 12-hour mission readiness test, using a representative activity timeline.

The result of this test was the discovery of a mission-critical flaw that would have prevented the recovery of the primary payload's data. This flaw could not have been corrected on-orbit.

Slide 94

## Test Design Required Elements (2)

- LYF Test design roles and responsibilities of organizations and personnel involved in test
- Added design considerations that must be accounted for
- Test inputs and their sources
  - *Use of stimulators, simulators, emulators and test equipment*
- Operational tools and processes that will be used
- Test tools, configurations, and processes to be used in planning, executing and evaluating the test
- **Independent and dependent variables for the test**
- **Test points to be monitored**
- **Test constraints/limitations**

***Note key deviations from mission inputs***

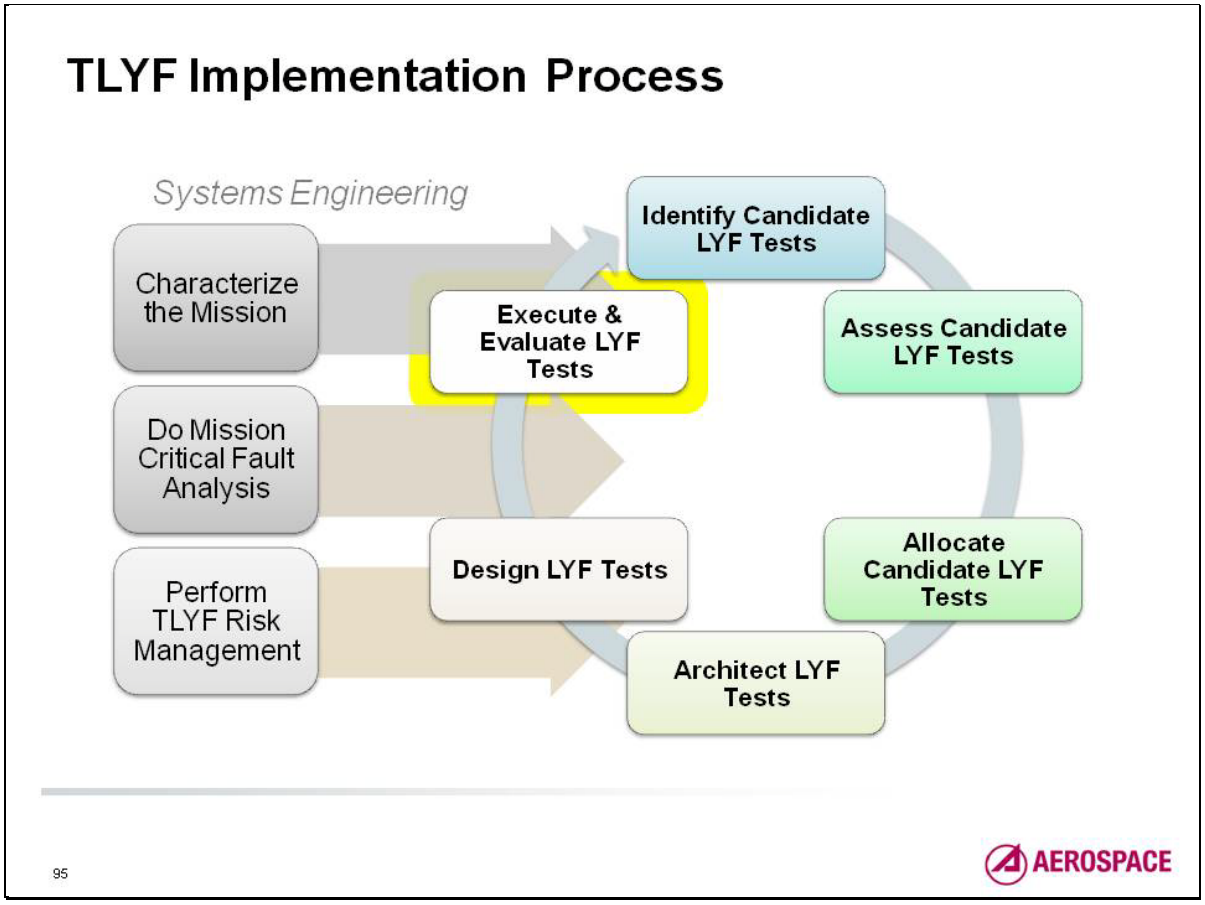
94

AEROSPACE

Test design roles and responsibilities for a LYF test are likely to be distributed across a team of people representing all the disciplines and elements involved. The team may include, but is not limited to: representatives from mission engineering, mission planning, command and control, system engineering, payloads, spacecraft systems, operators, and users. It is the responsibility of the test design team to: refine the test objectives, identify possible test cases and select cases to be included in the test, craft the test flow, identify test resources, identify test constraints, assign/review/manage the development of the test procedures, dry run the test procedures for discovery of test design problems, and execute the test procedures. It may or may not be the responsibility of the test design team to evaluate the test results. The TLYF test design team also has the responsibility for identifying which first time- and mission-critical events are actually covered by the test, which potential flaw paths are intended to be exonerated or discovered in the test, and what deviations from mission items and processes are notable in the test.

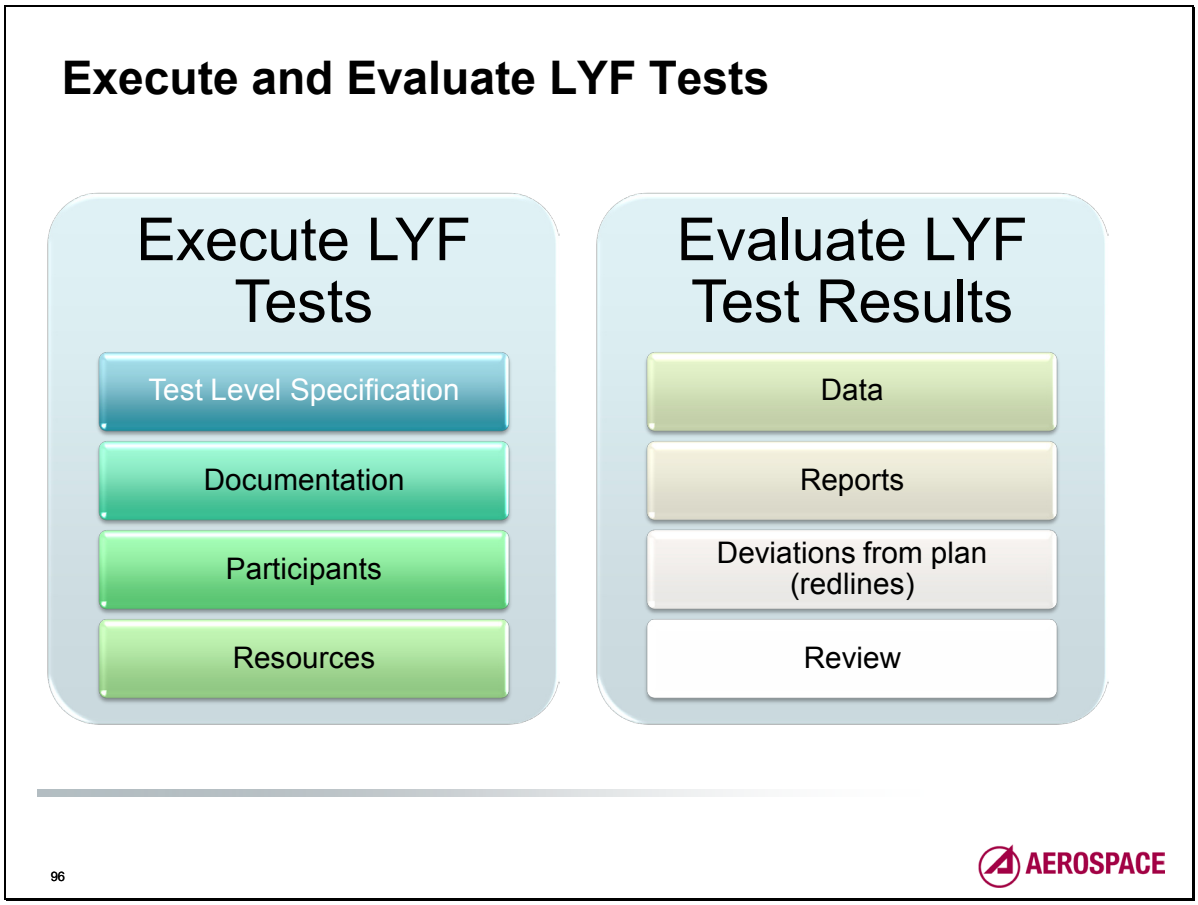
A multi-element LYF test is likely to need multiple test procedures and scripts, as each organization involved in the test will need to have the test procedure be equivalent to their mission execution products.

Slide 95



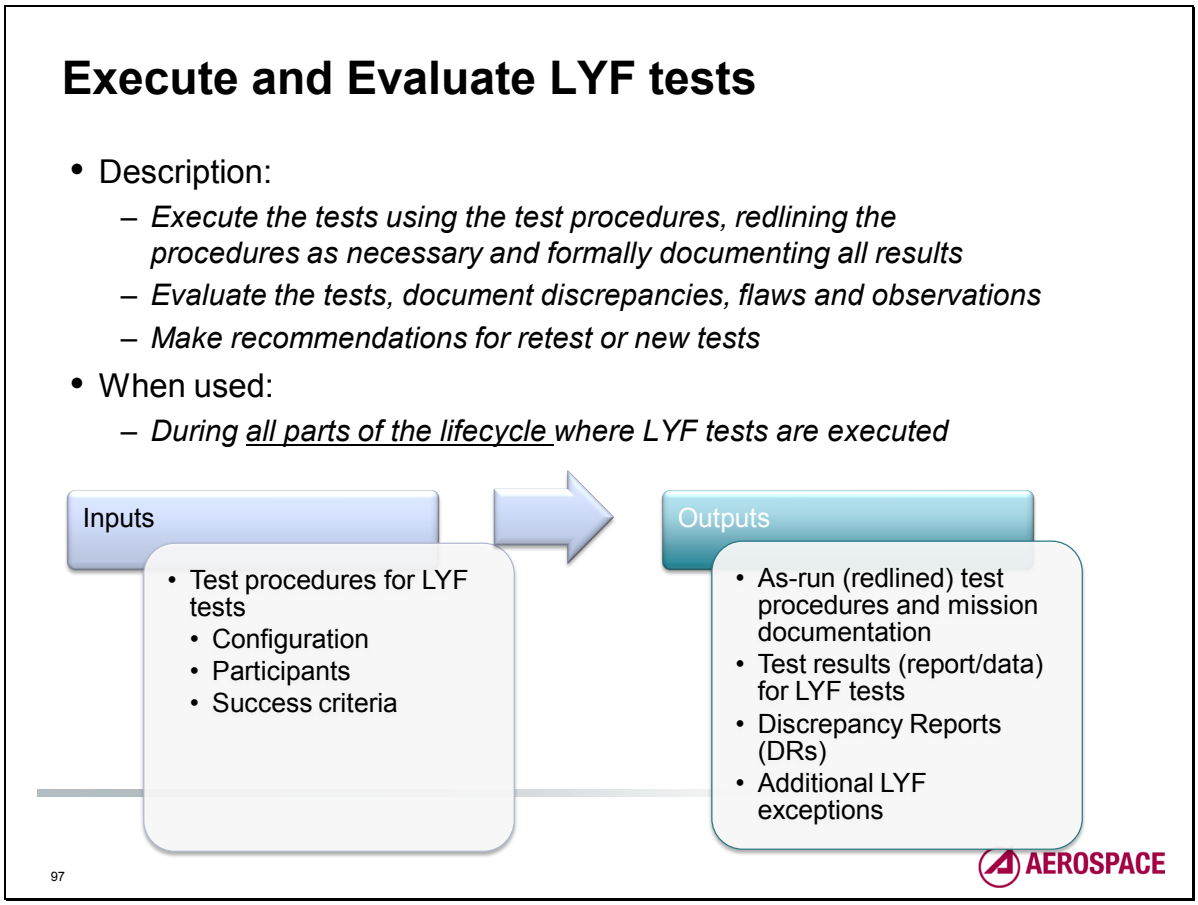

After all the planning, it's time to execute and evaluate each LYF test.

Slide 96




The execution of a LYF test has most things in common with the execution of any test of any portion of a space system. What differentiates the execution of a LYF test is how closely the test process emulates the set of mission activities encompassed by the test. During test execution all aspects of the mission activity must be captured and evaluated. When a spacecraft is tested in a factory setting for "traditional" tests, anomalies can occur due to a number of sources (test personnel, test software, and test equipment) that ultimately have little or no impact on how elements of mission may be affected. When a LYF test is conducted with ground personnel in place of test personnel, using mission procedures on ground control equipment, with mission-like data routed to users, every aspect may ultimately have a profound effect on how the mission will be run. This may call for a different level of coordination prior to and during the test execution, as well as some added facets to anomaly detection and resolution. Deviations from the baseline test plan must not only be noted, but must be evaluated for additional TLYF exceptions and for feedback into the way the system will need to be operated during the mission.

Slide 97




Test execution for a LYF test opens a discussion of how the test team should respond to unexpected behaviors and unpredicted outcomes. Traditional test execution will have protocols for stopping a test, troubleshooting discrepancies, or continuing the test when such revelations occur. When such revelations occur during a mission, different protocols are likely to be used, as it is not possible to take some paths that are available pre-launch. The test team must decide what kinds of discrepancies need to be handled by which protocols.

Similarly, the evaluation of the test as run may be made on the basis of inputs, outputs, products, and performance as it would be during the mission, or evaluated from non-flight test equipment. The former includes examination of realtime and stored telemetry, data products, and mission services. Anomalies should be identified from procedure execution, instantaneous health data, health data trends, examination of mission data or mission service performance, and mission process problems. The latter may be necessary to characterize flaws that cannot be detected directly by mission information.

Because many organizations may be involved in the highest level of LYF tests, the process for the identification, handling, and tracking of discrepancies uncovered during test execution must be in place prior to test execution. Failure review boards should have representation from all elements participating in the test. Final authority for discrepancy resolution must be clearly identified.

Slide 98

## Executing and Evaluating LYF Tests
### *Considerations*

- When does the (contractual) clock start for this test?
  - *Are dry runs considered part of the flaw detection activity?*
  - *They must be to evaluate the true effectiveness of the test*
- Who determines the degree to which the test is successful?
- What are the retest considerations?
  - *Is there a threshold of system, hardware, software, process changes as a result of test discoveries that warrant a retest?*



AEROSPACE

There are other considerations that may need to be addressed in conducting a LYF test. Preliminary execution of a test procedure (dry run) is frequently done to validate the correctness of the test procedure, but it is likely to also be an early chance to detect problems with the items under test. There may be a temptation to fix them and move on with the dry run, rather than using a more formal method of discrepancy handling. The case for using the more formal methodology is to ensure that all participants maintain an awareness of the system's responses, as they may have ramifications in other elements involved with the test. These discoveries may also need to affect the way in which the mission is conducted.

LYF tests, which are used to demonstrate readiness to proceed to the next milestone, need to be evaluated by those responsible for architecting the test and those responsible for the activities of the next milestone. LYF tests that are used as risk reduction need to be evaluated by those involved in risk management, as well as those directly connected with the test.

Most major tests engender high visibility discussions about the need to perform a retest following removal/replacement/revision. A LYF test must be examined from the "test what you fly" principle. Changes to the system as a result of test revelations may have unintended consequences at the integrated level that cannot be seen in lower level tests. Changes that fix the first problem may make it possible to discover flaws that couldn't be seen until the first problem was eliminated. These are lessons from earlier mission failures that should drive retest considerations.

Slide 99

## The Value of a TOCT/WITL Test

- This is conducted late in the test flow, prior to shipping SV to launch base
- Those who do this test consistently find mission degrading anomalies well after all requirements-centric testing has been completed
  - *Most of the anomalies found were software related*

### Table 1: Anomaly Detection Summary*

| Buyer | Prime Contractor | Space Vehicle | No. of Space Vehicles | No. of End-to-End Tests | Mission Degrading Anomalies Detected/ Test |
|---|---|---|---|---|---|
| NASA | JHU/APL | MESSENGER | 1 | 5 | 6.2 |
| NASA | JHU/APL | New Horizons | 1 | 4 | 9 |
| ESA | Various | Various | 20 | 40 | 2.6 |
| USAF | Boeing | ARGOS | 1 | 1 | 3 |

* *End-to-end Testing In A Test Like You Fly Context*, Julia White and Charles Wright, The Aerospace Corporation, 23rd Aerospace Testing Seminar, October, 2006

99

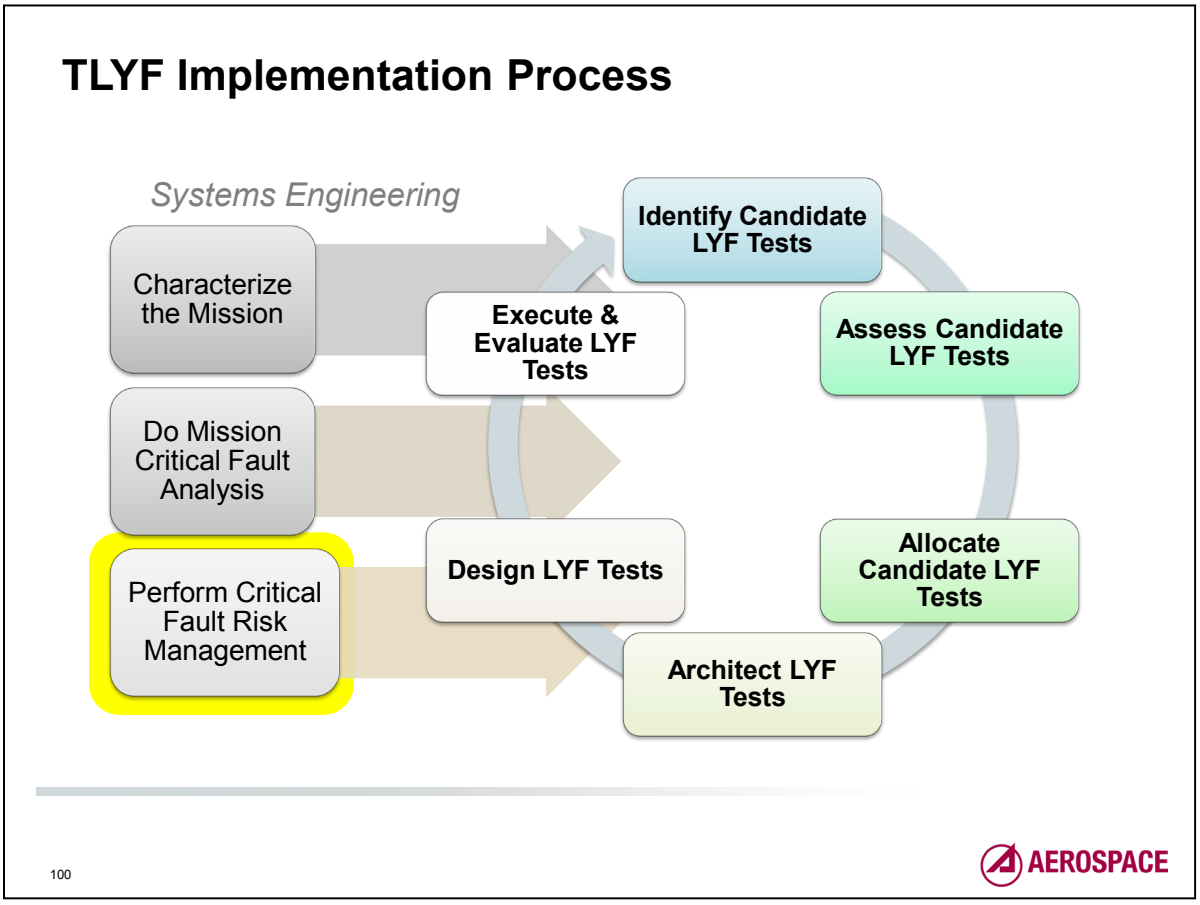
AEROSPACE

The table shows the results from an examination of the outcomes 50 total operations chain (TOC)/week in the life (WITL) testing performed on 23 space vehicles. TOCT/WITL test detects between 3 and 9 mission degrading anomalies per test with a test weighted average of 3.6 anomalies per test. This data shows that the TOCT/WITL test has a comparable effectiveness for finding flaws as a space vehicle thermal vacuum test which has the highest effectiveness (4 – 6 MDAs) of any environmental test as reported by Charles P. Wright and Bruce L. Arnheim (*Insight into the Value of the System Level Thermal Vacuum Test*, 21st Aerospace Testing Seminar, 2003). It must be emphasized that the TOCT/WITL tests are run after requirements verification activities, including interface checks and compatibility, have been completed. This test finds anomalies that cannot be found by other forms of testing.

The European Space Agency (ESA) requires (*Space Engineering Testing, ECSS-10-03A*, ECSS Secretariat, ESA-ESTEC, Nordwijk, The Netherlands, February 2002, para. 4.9.5.3) this test be run *directly* with the space vehicle linked to the ground station. This largely proscribes the use of space vehicle software simulators in the End-to-End test, thus meeting the Test What You Fly aspect. ESA defines two TOC tests and when they should be run referenced to the launch campaign (6 and 3 months prior to launch). Guidance is also given regarding the length of the tests: between one and two weeks each using "realistic operations sequences," much of which is done on a mission timeline.

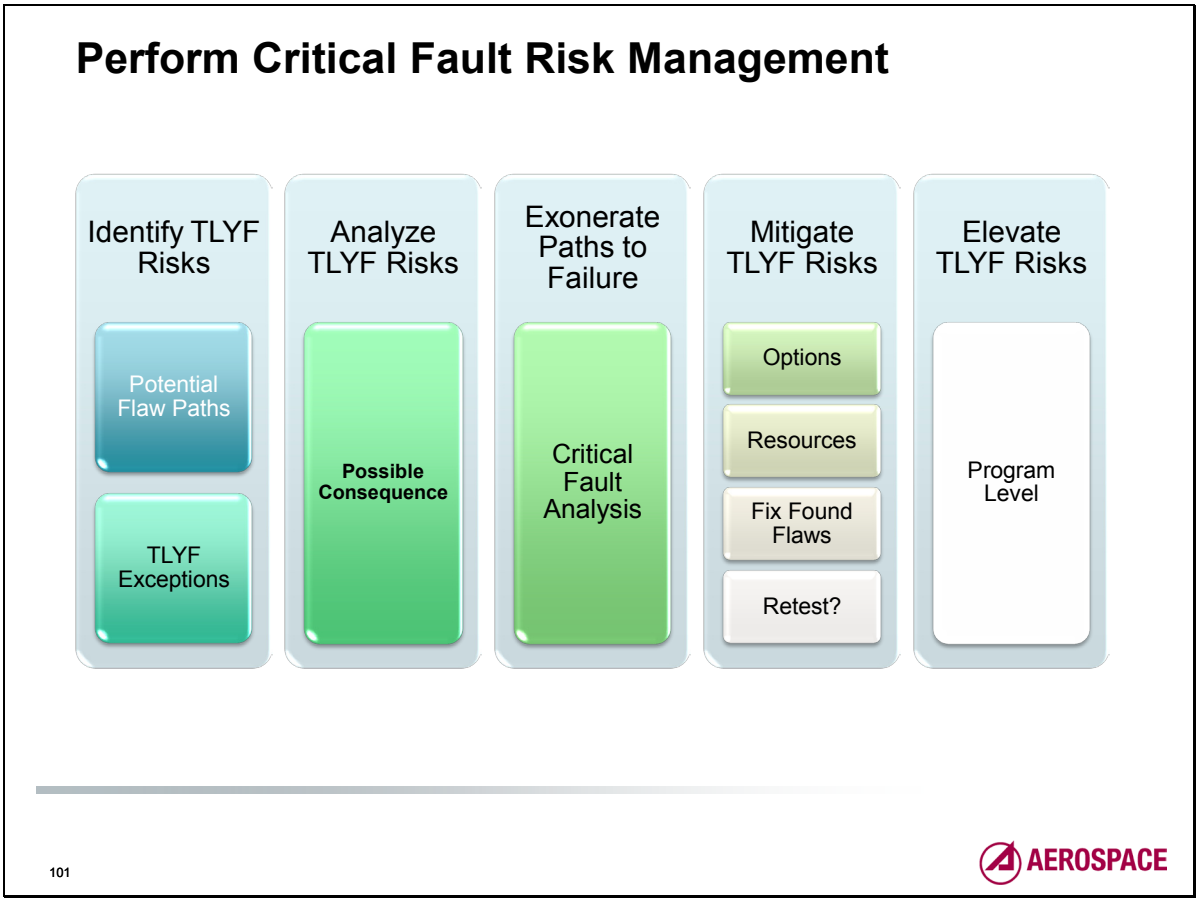
Lessons learned shows that mission degrading anomaly escapes are reduced with the application of the TLYF philosophy by the acquisition team when they require flight-like test, or a series of tests, to occur at the highest level of integration (total operations chain) to validate mission readiness prior to launch, with lower levels of tests as needed for practicality, resource optimization reasons, or risk reduction.

Slide 100




Critical Fault risk management is executed throughout the TLYF implementation process to ascertain the adequacy of the TLYF program. It is listed as the last step, because it is the end of the process: when the risk of critical flaws have been handled, accepted, exonerated, or revealed and repaired.

Slide 101




The heart of Critical Fault risk management is identifying critical faults that could cause mission failure. The TLYF plan is one way of exonerating such flaws. The TLYF exceptions list will help assess whether the LYF tests will be perceptive to the flaws.

If the planned tests are not perceptive to a given critical flaw, the risk management process will devise a plan to reveal or exonerate the flaw. If the plan is not executable within the available resources, the risk is elevated to the program level so that either additional resources can be provided, or the program KNOWINGLY accepts the risk of a potentially fatal flaw.

Slide 102

## Critical Fault Risk Management

- Description:
  - *Encompasses identification, analysis, mitigation planning and implementation, monitoring, and elevating critical fault risks*
  - *Identify mission critical risks based on*
    - Potential flaw paths to mission critical failure situations, as an output of the critical fault analysis
    - **Exceptions identified during the LYF test design process**
  - *Perform fault analysis for identified exceptions*
  - *Exonerate each potential path to failure, or provide evidence of the nature of the discovered (actual) flaw*
  - *Mitigate discovered flaws*
  - *Elevate critical fault risks that cannot be exonerated within allocated resources*
- When used:
  - *Continuously throughout the acquisition lifecycle*

102

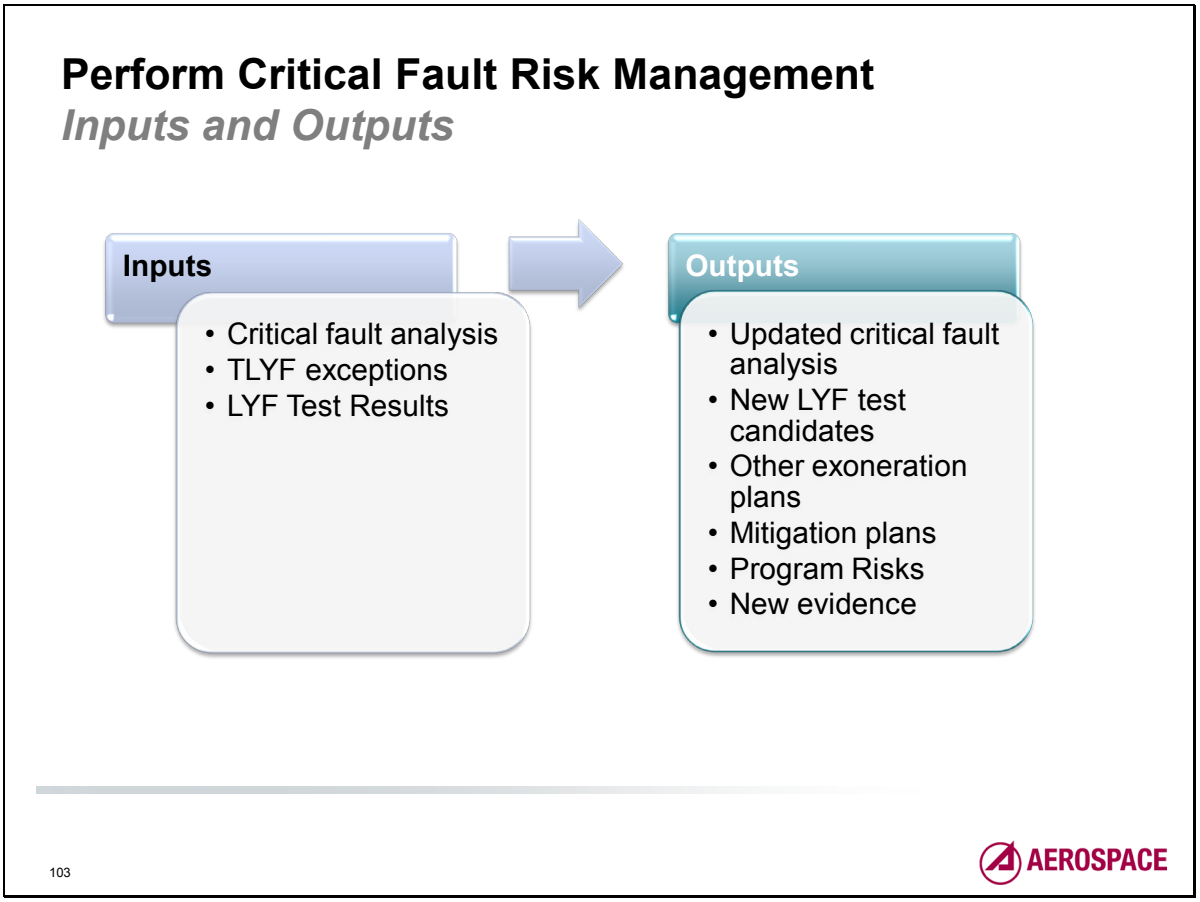
AEROSPACE

Defining and managing a *TLYF* exceptions list is a part of the program overall risk management effort. Implementing *TLYF* requires the assessment of the risks of both testing and not testing *Like You Fly*. What cannot or will not be done must be managed as well as what can be done. Identify the risks associated with a TLYF shortfall and compare them to the risks associated with doing a test in a TLYF manner. This is necessary to have an informed decision-making process. These risk assessments will be done in a slightly different manner and format than program level risk management initiatives. Most of the mission-ending anomalies that are traced to the lack of *Like You Fly* testing had neither engineering nor management visibility into the trade-offs involved in the test approach. A failure that occurs when the risks are understood is much more palatable, as everyone in the chain involved in the decision understands what the options were.

TLYF Exceptions: Managing What You Do Not Do

A "LYF test exception" is a known difference between a characteristic that will be present during the mission and the equivalent characteristic as implemented during the test in question. It may be that the characteristic cannot be included at all or it may be an approximation to the characteristic. The intent of identifying a LYF test exception is to raise the question: by not including this characteristic in this test, or by including a particular approximation of that characteristic, will the test be likely to miss a mission-critical flaw? Because there are potentially dozens, if not hundreds, of mission characteristics that could be identified for any mission activity or sequence of activities, there needs to be some method for identifying those exceptions that are most likely to mask a flaw that will be present in the actual mission execution. That method is the mission critical fault analysis.

Slide 103




Taking the results of the critical fault analysis, TLYF exceptions analysis and LYF test results, the Critical Fault risk management assesses what critical faults may still exist within the system. For each such fault, an exoneration plan should be devised. This plan may include, but is not limited to, a LYF test.

Slide 104

## Lessons from Hubble Space Telescope

*Everything You Wanted to Learn About TLYF*

NASA


*Photos Courtesy of NASA/Space Telescope Science Institute (STScI)*

- **Lesson:** Conduct end-to-end tests of integrated equipment
- **Lesson:** Apply LYF test technique to new parts

**Lesson:** Identify and mitigate risk*

*"The Project Manager must make a deliberate effort to identify those aspects of the project where there is a risk of error with serious consequences for the mission. Upon recognizing the risks the manager must consider those actions which mitigate that risk."*

** The Hubble Space Telescope Optical Systems Failure Report, NASA, November, 1990*

***Initial severe degradation to mission***

104

AEROSPACE

**Incident Summary**

Shortly after its 04/24/90 launch the Hubble telescope was found to have a defect, which was spherical aberration (which reflects light to several focal points rather than to one) of the primary mirror. The mirror was polished too flat by 2.3 microns (about 1/50th of the width of a human hair), a mistake not caught on the ground primarily because the same manufacturing equipment responsible for the error was also used for verification.

The optical flaw that was embedded in the original Hubble telescope is one of the leading inspirations to develop the TLYF assessment process that includes a risk-based assessment process. A full end-to-end optical test of the integrated telescope would have discovered the flaw almost immediately. This test was not run due to its high cost, although the cost of the test was much less than a shuttle service mission to fix the flaw. In the absence of such a test, there was some effort expended by program management to convince themselves and higher NASA management that all parts of the optical train were manufactured and assembled according to requirements. The potential existence of the flaw was known by some of the technicians at the time. The data that proved the existence of the flaw was available prior to flight. An independent evaluation of the telescope, pressured for a quick assessment, was included as part of the readiness activities. And yet this mission-critical flaw escaped to orbit in spite of these steps. The primary lesson identified by the failure investigation team was the need to "identify and mitigate risk." In other words, program resources need to be applied in direct proportion to the risk of otherwise missing potential flaws that prevent the execution of the mission. In the absence of an evaluation of criticality, every aspect of program development and independent review are treated equally. Limited program resources need to be applied to those items with the largest potential impact to the success of the mission.

Slide 105

## Program Risk Management (RM) vs TLYF RM

*Distinctions*


- Based on a methodology that uses likelihood (probability) as part of the risk ranking process
  - *Allows mission critical consequences to be downgraded by perceived low probability of occurrence*
- Focus is generally on mitigating risk level by lowering probability, e.g.
  - *Having back-up plans*
  - *Changing thresholds*

- Based on a methodology that actively seeks the "one strike and you're out" kind of flaw that would prematurely end or seriously degrade the mission
  - *Keeps focus on criticality of consequence*
  - *Puts probability in terms of a coin flip (flaw either exists or not)*
- Focus is on exonerating potential path to failure (no flaw) or validating existence of flaw
  - *A found flaw is a realized risk – a fact, not a possibility*

**Virtually all mission ending or critical flaws would have been identified as "low likelihood" pre-launch - They happened anyway!**

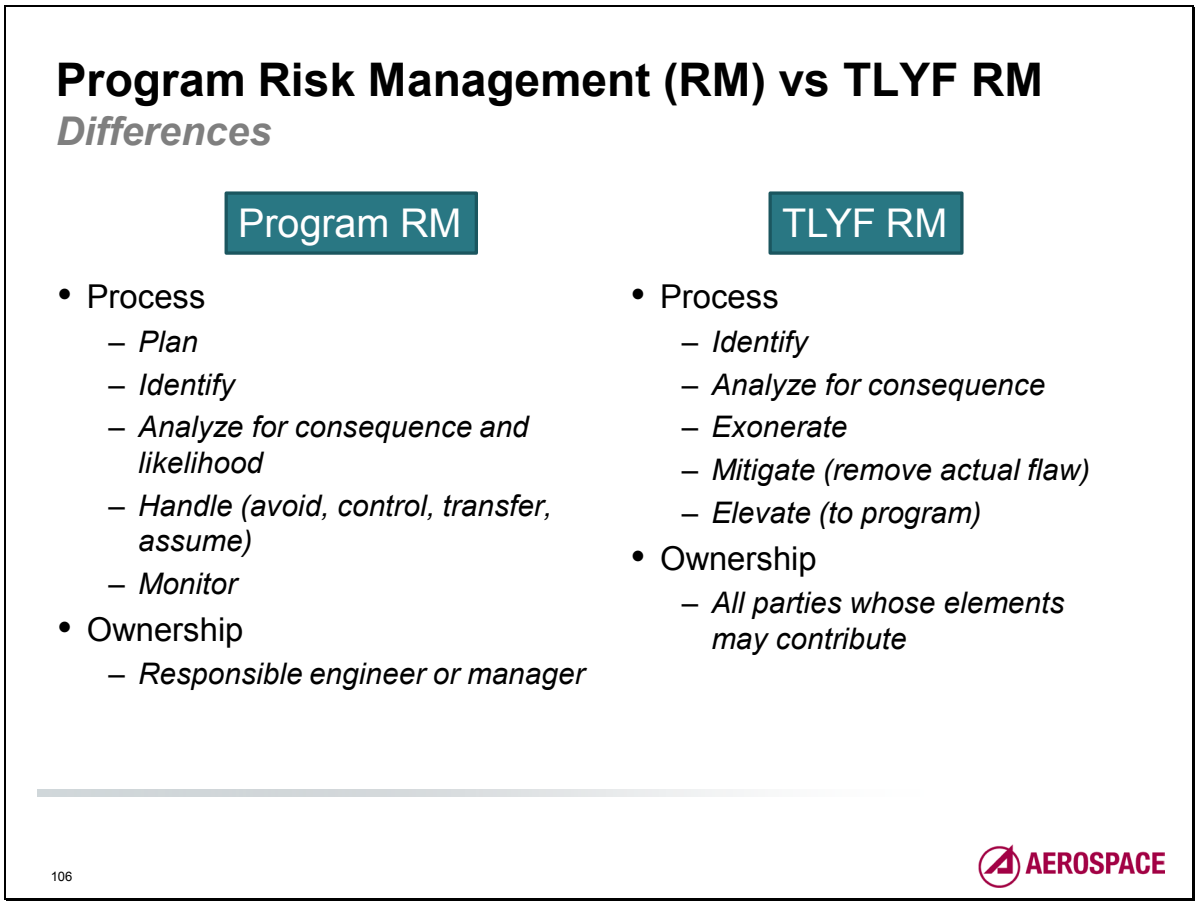
105

AEROSPACE

The domains of program risk management and critical fault risk management are fundamentally different. During development, risk management deals with those things that can disrupt program execution, including budget and schedule, as well as technical performance, and considers both the consequence and the probability. For instance, a programmatic risk might be that a particular technology is not ready for insertion into the program. If the probability is low, the program may choose to simply monitor development of the technology. If the probability is higher, and the technology is critical for mission success, the program might introduce mitigation measures such as adding resources to accelerate development or to provide a back-up.

TLYF focuses on flaws to execution of the operational mission. For a given potential flaw, the consequence is either minor (green), moderate (yellow) or critical (red). Since critical flaws can cause mission failure, it is crucial to consider how to exonerate or reveal such flaws. Many mission-ending flaws would have been identified as "low likelihood" prior to launch. In fact, they were often the result of several errors, including poor communication, that are difficult to identify within the usual mission assurance process. And this is why it is not appropriate to use probability in the critical fault risk assessment, as the existence of any critical flaw in actuality only has two possibilities: either the flaw exists or it doesn't. The key to critical fault risk management is to concentrate first on criticality, and then on exoneration or discovery.

Slide 106




The process for managing program execution risk and mission execution risk differ in fundamental ways. Program risk management has to include the items that can prevent a program from getting to launch, while TLYF has a much narrower, technical focus on those things that prevent operational success. Critical fault risk management strives to identify potential fatal flaws, exonerate or reveal the flaws, and remove the flaws that are revealed. LYF tests are one method by which a given flaw may be revealed or exonerated, but it is not the only method that can be used. When a given flaw cannot be exonerated within the available program resources, the risk should be elevated to the program risk management process.

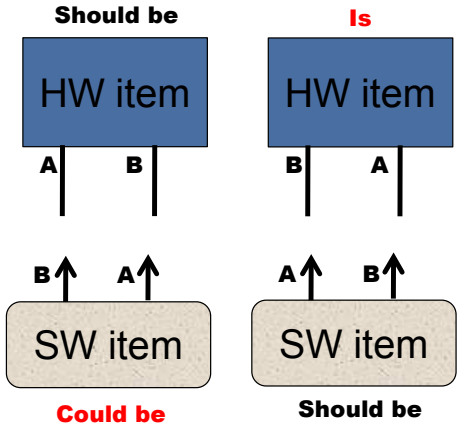
The LYF test creation process assumes that it is done within the allocated test resources. Resources needed to exonerate some flaw paths may exceed available resources. Elevating the critical fault risk to program RM provides opportunity for additional resources.

Slide 107

# Exonerating Potential Paths to Failure

## *Example and Considerations*

- "Like You Fly" generally implies interactions and concurrency of characteristics
  - *Fault analysis must address these*
  - *Exoneration must apply to contributors*
- It's not enough to show that hardware matches schematic
  - *Must provide evidence that there are no flaws affecting the interacting HW and SW*

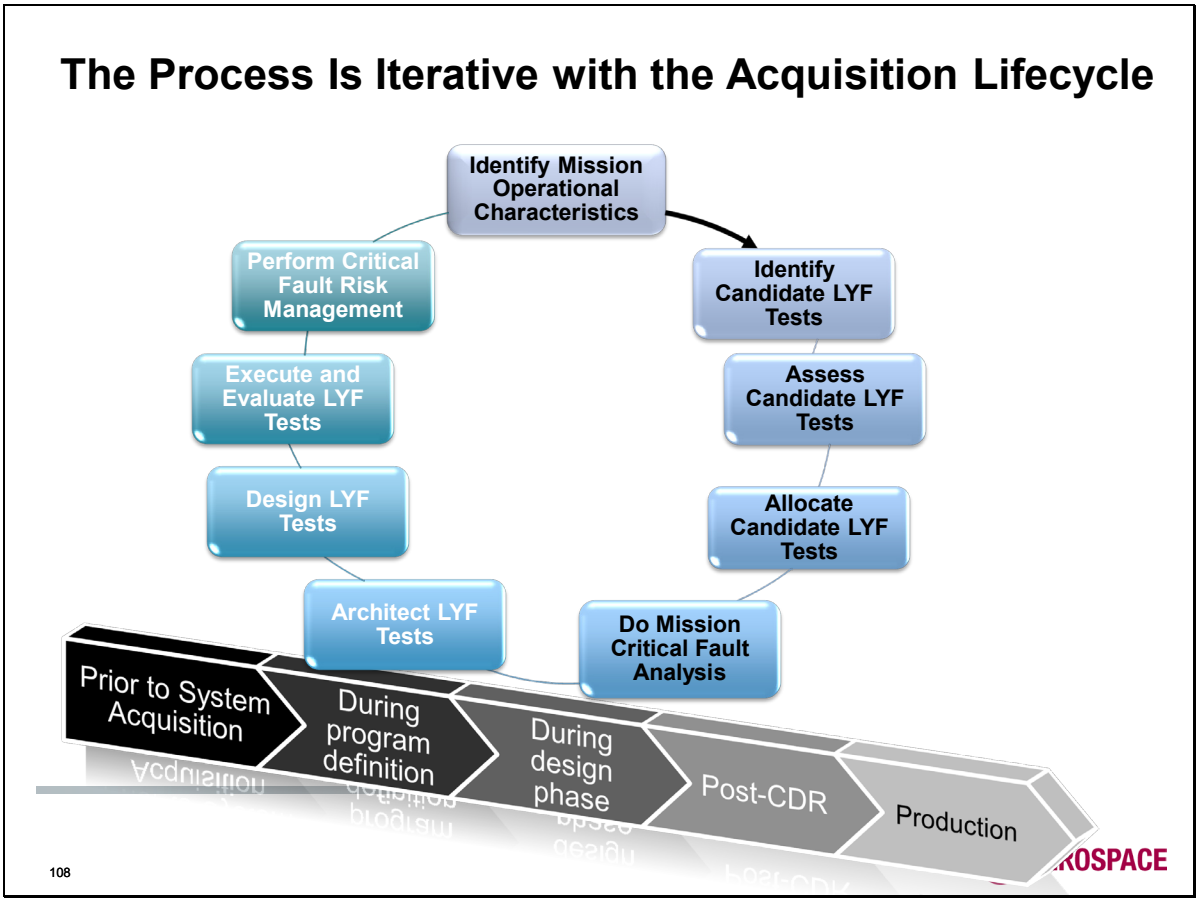



107

AEROSPACE

It is crucial that the identification of potentially fatal flaws occur at the integrated system or enterprise level and that the exoneration path include sufficient scope. A common problem is to restrict such analysis to within each subsystem, which can miss critical interactions between subsystems.

Slide 108




The earliest iteration occurs during acquisition planning, as there are acquisition decisions that must be made to allow adequate and appropriate LYF tests to be developed for validating mission executability and readiness. Iterations are necessary as a better understanding of the system will provide more insight into first time- and mission-critical events, additional failure situations, more potential paths to failure, and better definition of the mission phases and timelines.

Slide 109

## Adding LYF Testing Later in the Life Cycle

- Before CDR
  - *Can do all of process*
  - *May need definition and resources for additional scope*
- After CDR
  - *Know the Mission: It's never too late to create a 1st time/mission critical events list*
  - *Mission Readiness: It's never too late to add a Total Operations Chain Test - Days/Weeks in the Life test*
    - Might not be as complete as one designed earlier
    - May be possible to leverage existing tests
  - *Critical Fault Analysis: Leverage design work already done for AFM and contingency planning*
  - *Critical Fault Risk Management: Prioritize testing based on risk*

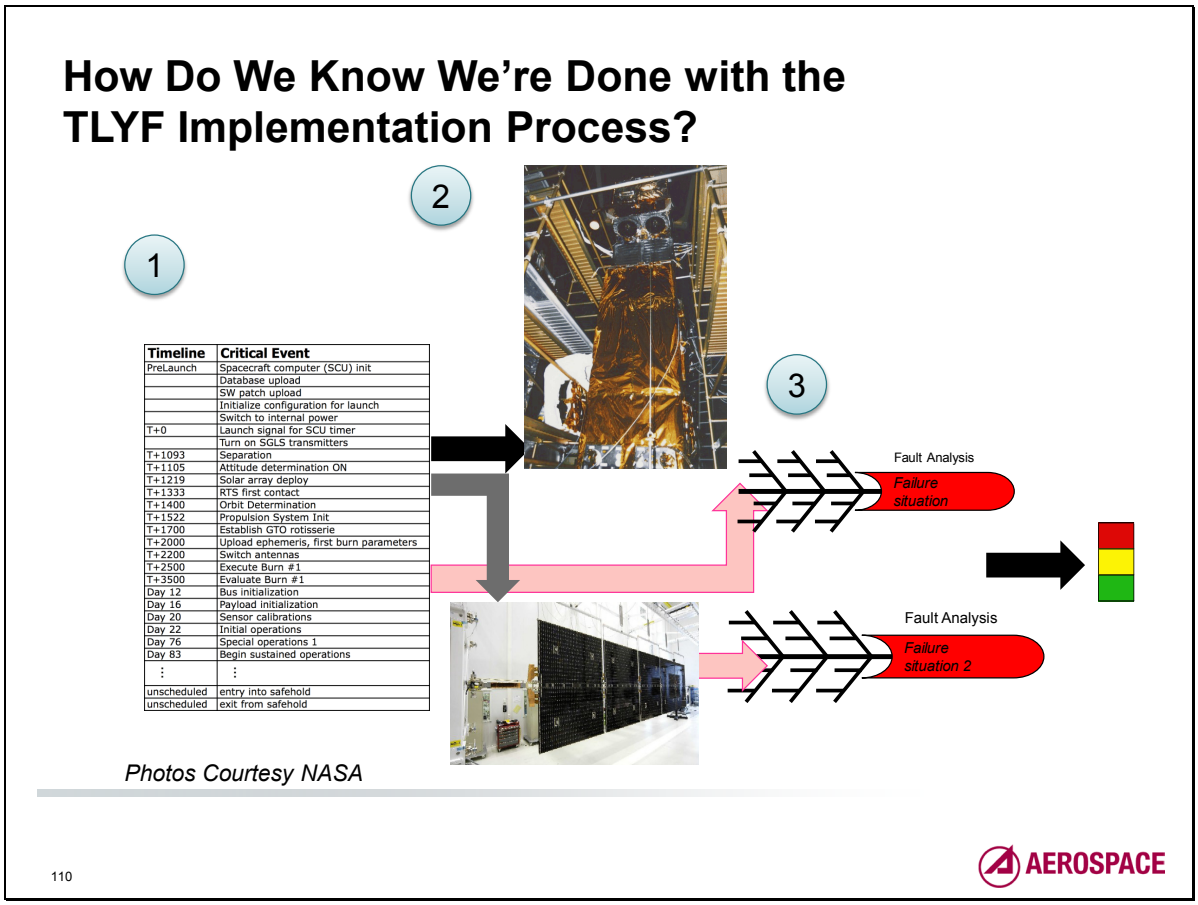
109

AEROSPACE

Those programs that are still in the design phase have the opportunity to do the full TLYF implementation process. What is likely to suffer is that specific resources to support LYF tests may not be available within program constraints. This is likely to lead to fewer LYF tests, missed opportunities for LYF development tests, LYF tests of lower levels of hardware, lower fidelity of mission emulation leading to a higher number of LYF test exceptions, and a missed opportunity to align ground and space segment development for common equipment and software.

After CDR it will not be possible to allocate LYF tests to the lowest levels for perceptivity and risk reduction, unless there are additional vehicles being built in the acquisition. These missed opportunities must be examined carefully for potential critical flaw escapes. There will be fewer program resources available for LYF tests. There are likely to be severe constraints on running LYF tests due to the lack of development of supporting equipment and software.

Slide 110




The TLYF implementation process is not open-ended. It starts with a list of first time- and mission-critical events, and an identification of mission phases and activities. Candidate LYF tests are identified, assessed, and allocated to the test program. A mission critical fault analysis is used to focus attention on potential mission fatal flaws. All identified mission critical failure paths are either exonerated or revealed and mitigated. Those critical paths that cannot be exonerated or revealed as part of normal program resources are elevated as a program risk and handled within risk management resources or accepted by the full acquisition community.

## TLYF Process Development Status/Way Forward

- The TLYF Assessment/Implementation Process is a work in progress
  - *TLYF Guidelines*
  - *SMC TLYF "Policy" and subsidiary documentation*
  - *Air Force/SMC Instruction (Test and Evaluation) revision*
  - *TLYF Handbook*
  - *MAIW 2009 TLYF "checklist for SV in high bay"*
  - *TLYF Government/Industry Community of Practice*
  - *"MIL-STD-1540E" revisions*
- Need to gain experience with process before establishing standards
- Need to understand differences, if any, for different mission classes

*A Team Sport*

111

AEROSPACE