The Test Like You Fly (TLYF) Or Use or Operate Implementation Process

Overview

Julie White
System Integration and Test Office
The Aerospace Corporation
(310) 336-4047
Julia.D.White@aero.org

Lindsay Tilney
System Integration and Test Office
The Aerospace Corporation
(310) 336-7104
Lindsay.G.Tilney@aero.org

August 17-18, 2020

Approved for public release. OTR 2020-00812.

Desired Learning Objectives

- **As a result of this overview, attendees will be able to:**
  - *Understand the value of applying the TLYF process in the context of systems engineering and mission assurance*
  - *Describe the TLYF process implementation steps and expected results and products*
  - *Gain awareness of the power of of deriving tests from successful mission execution and from an awareness of potential fatal flaws*

Questions for Class

- **About you…**
  - *Technical specialty*
  - *Organization*
  - *Mission area*

- **Expectations…**
  - *What to do you hope to obtain as a result of the tutorial?*

Q

Test Like You Fly – Background

- **Hard and expensive lessons have driven the formulation of the Test Like You Fly (TLYF) process**
  - *A string of mission failures occurred in the 1990s and 2000s*
  - *The post-mortem failure investigations produced lessons*
  - *Alternate processes are needed to catch flaws preflight*
  - *These failure lessons have helped form the steps we put into the TLYF Process*

- **Post-mortem analyses of failed missions show that systems were not being tested in an operationally realistic manner**
  - *These test deviations from operational realism have led to loss or degradation of mission*

Test Like You Fly – Background

- **Historically, typical systems engineering practices utilize testing as a method to verify requirements**
  - *Validation of the concepts of operation have had less emphasis*

- **Requirements verification is necessary, but insufficient**

- **Demonstrating that a system can successfully perform its mission (deliver mission products or services) is fundamentally different than demonstrating that the system meets requirements**

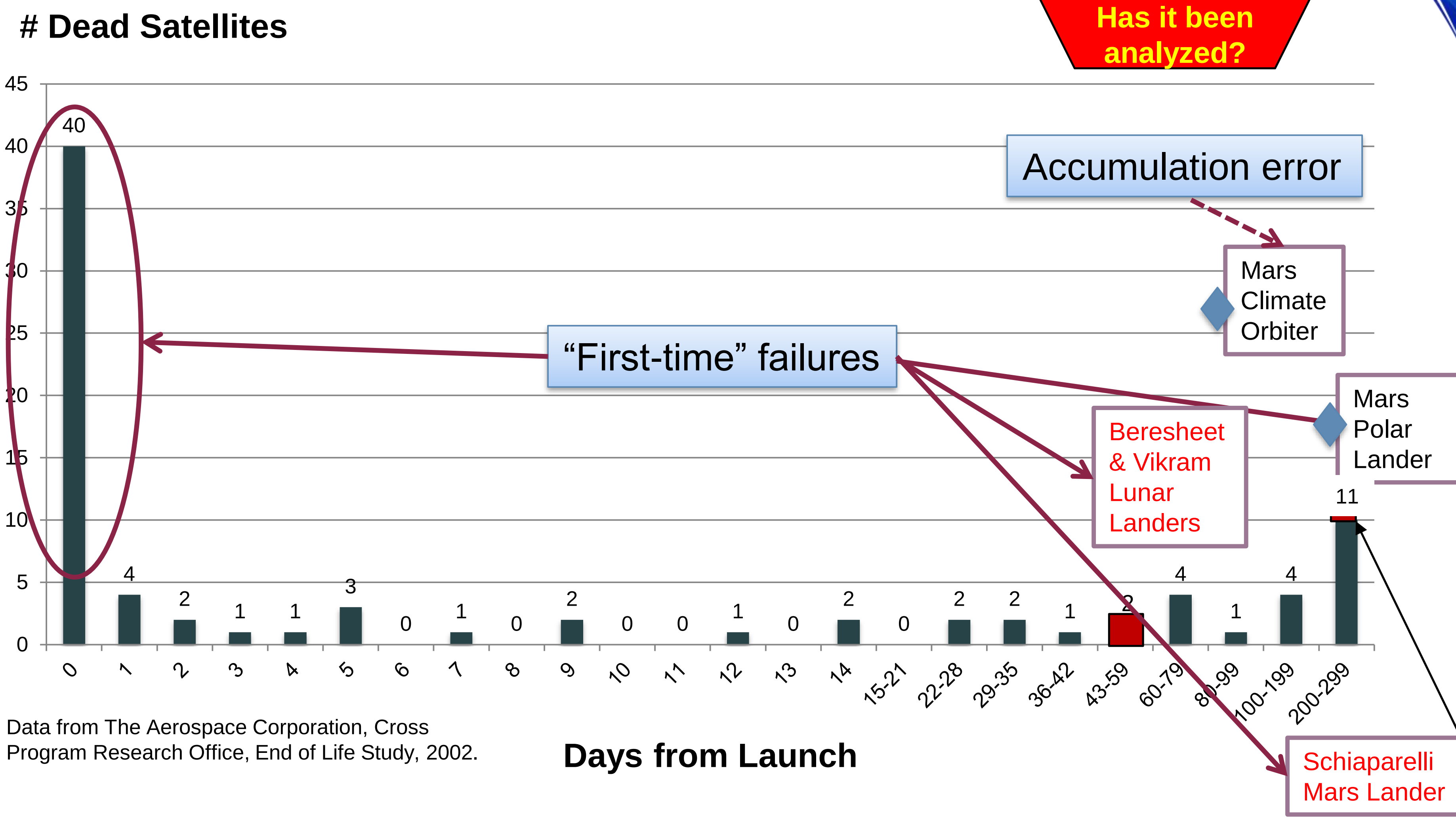
- **Tests performed under…**
  - *non-mission conditions (e.g., mission sequence, timeline, concurrency, etc.)*
  - *with non-flight hardware (HW) and/or software (SW),*
  - *with incomplete or previous (pre-repair) configurations, or*
  - *without the last preflight SW build/version*

  -> will miss the flaws that can only occur under mission conditions.

Lessons from Historical Failure Data

Many of the Earliest Losses are TLYF Escapes

Do you have project / industry failure data? Has it been analyzed?



Data from The Aerospace Corporation, Cross Program Research Office, End of Life Study, 2002.

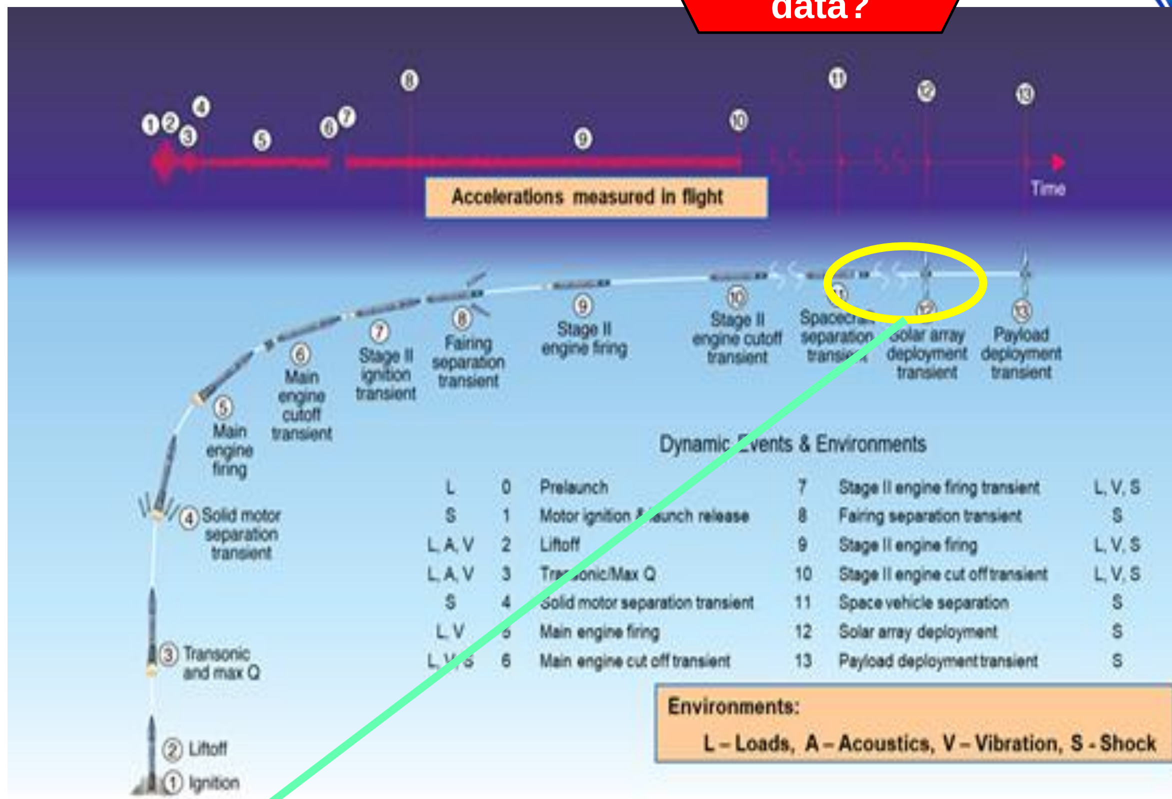
Losses prior to 100 days are frequently test escapes.

First Day Space System Failures

May Involve Many Elements

Is there a common theme in your failure data?

- **Failure to become power positive**
- **Failure to become attitude stable**
- **Failure to communicate with command & control**
- **Vehicle acquired in off nominal conditions**



Notional Functional Flow Diagram for Auto Initialization

Detumble → **Find the Sun** → **Become Power Positive** → **Orient SV for Comm** → **Initialize for Comm**

The Necessity for Testing "Like You Fly"

Lessons Drive the Process

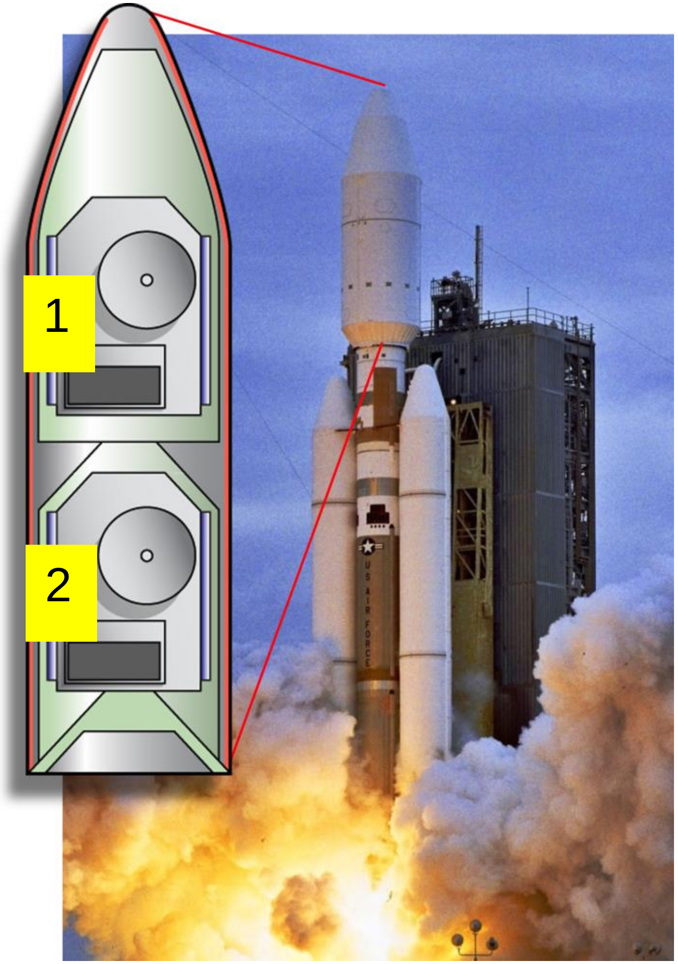
Can you draw general lessons from project failure data?

Vehicle	Year	Mission-Critical Anomaly Root Cause	Result
Titan CT-2 Launch	1990	Miswiring prevented satellite separation; Ground test using non-flight software did not identify the problem.	**Loss of Mission**
ESEX Payload	1999	Exploded in space after leaking battery electrolyte caused short circuit; battery qualified in non-flight condition	**Loss of Mission**
Mars Polar Lander	1999	Faulty touchdown sensor logic caused vehicle to crash; Test not rerun with hardware and software after modification.	**Loss of Mission**
Mars Climate Observer	1999	English-Metric units error crept into modified software; Software being deemed non-critical, was never tested.	**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	**Loss of Mission**
TERRIERS	1999	Torquer coil installed upside down; Hardware and software never tested together.	**Loss of Mission**
Milstar 2-F1 Launch	1999	Improper filter coefficient loaded into flight software; No validation of filter constants actually flown.	**Loss of Mission**
Genesis Return Capsule	2004	Four deceleration switches installed backwards causing parachute failure; Never tested in flight configuration.	**Significant Loss of Science Product**

Lessons from Titan CT-2

Assess Differences between Current & Previous Missions

- 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 & differences***
- Lesson: Test How You Fly
  - ***Test across mode and phase transitions***



Courtesy of NASA

Loss of Mission

“What we have here is a failure to communicate”

Words matter

Test Like You Fly

Test Like You Fight

Mission-Like Testing

Test Like You Operate

Fly What You Test

Weeks in the Life Test

Week in the Life

Operational Testing

Environmental Test

Day in the Life Test

Vignette Testing

Orbit in the Life Test

Days in the Life Test

Test as You Intend to Fly

Operationally Relevant Test

Fly As You Test

Scenario Testing

Test What You Fly

Thermal Vacuum Test

Mission Scenario Testing

Acoustic Test

Test As You Fly

Thread Testing

End-to-End Test

Like You Fly Tests

Reference Orbit Test

Operationally Realistic Test

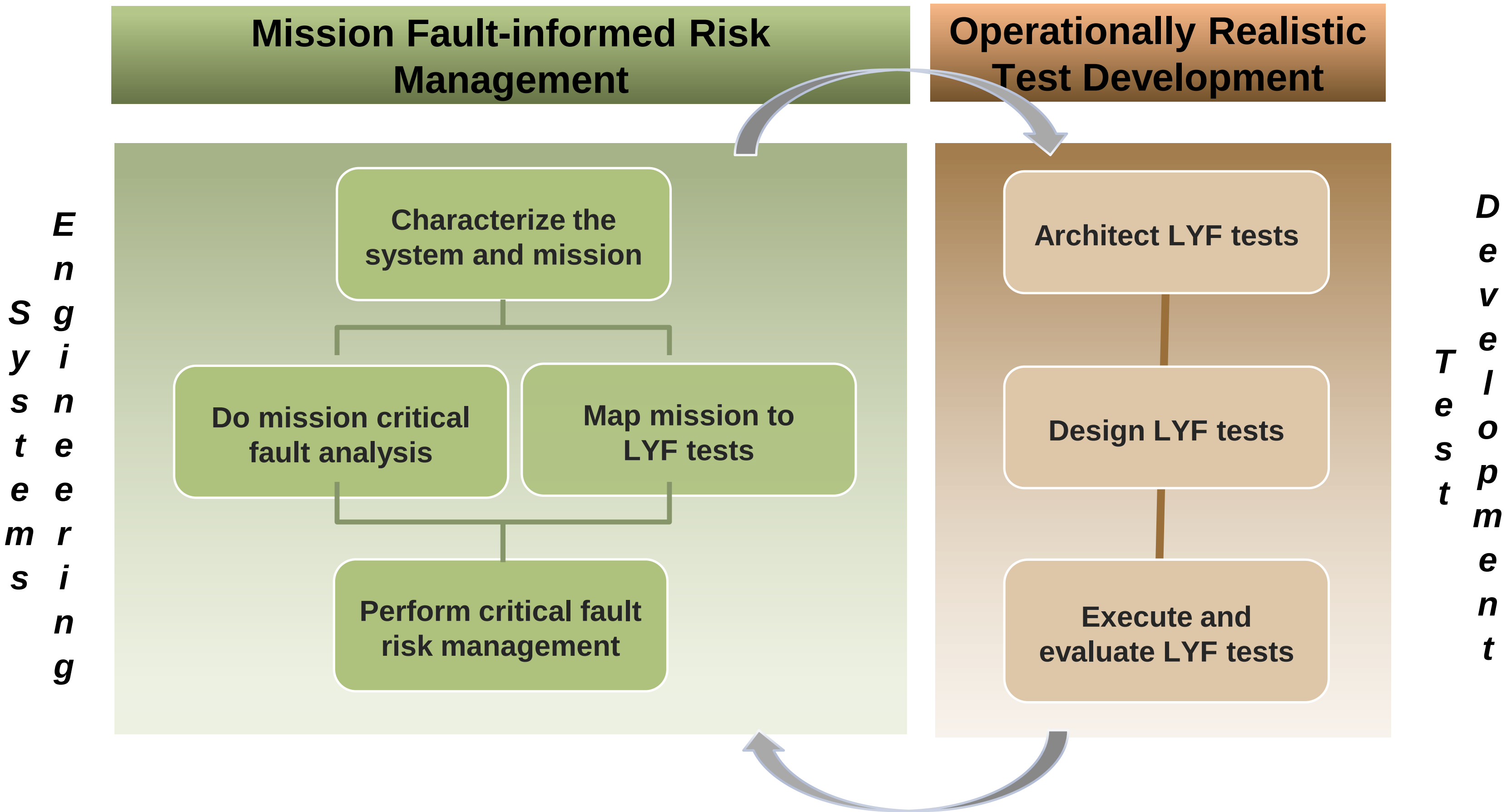
Mission System Testing

Use Case Testing

Functional Test

TLYF Process Implementation*

Systems Engineering and Test Development Interaction



The systems engineering and test aspects of the TLYF process are distinct, and the TLYF steps are placed into the appropriate disciplines

**TOR-2014-02537-REV A - The Test Like You Fly Process Guide for Space, Launch, and Ground Systems, Julia D. White and Lindsay G. Tilney, September 30, 2016*

Test Like You Fly—The Implementation Process

Definition

- *Test Like You Fly* is a prelaunch/pre-operational systems engineering *process* that translates mission operations concepts into perceptive operationally realistic tests to detect latent mission-critical flaws and assesses the risk of missing those flaws when it is not feasible to do those tests or adequately represent key mission characteristics while executing such a test
  - *The TLYF process is a comprehensive approach to validate a system's capability to perform the mission prior to launch or fielding*
  - *The TLYF process goes beyond the test domain; it also relies heavily on systems engineering disciplines*

- "Like You Fly" testing is a method to find flaws in the actual system to ensure its ability to perform the mission post-launch / post-deployment

The TLYF process results in operationally realistic "like you fly" (LYF) tests that address potential mission-critical flaw paths and contributors

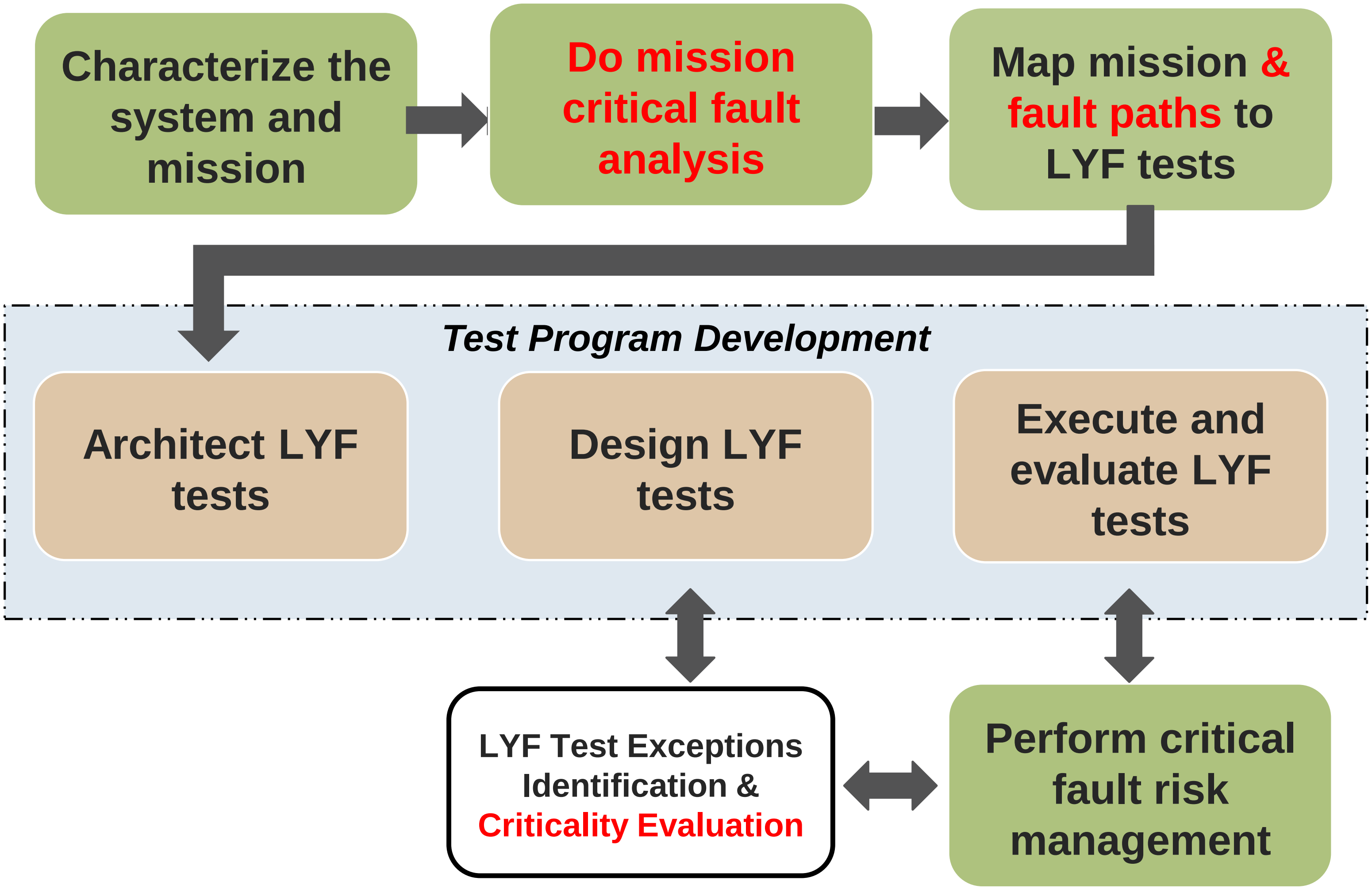
Key Definitions

Do you think in terms of your "mission" or your customer's mission?

- **Mission Characteristics**
  - *Operationally realistic characteristics include all aspects for mission operations/execution in terms of components, conditions, interfaces, transitions, transactions, processes, and environments. Typical mission* ***characteristic classes**** *are 1) end-to-end configuration, 2) time, sequence, and timeline, 3) environments (internal, ascent, space, command, ground and telemetry), and any relevant operational conditions that are present during the mission (people, processes, procedures).* **** Different for other mission areas***
- **Mission Coverage**
  - *Consists of phases, transitions, environments, and events in an end-to-end system configuration (i.e., combination of hardware/software and data when functioning as an integrated system), accepting nominal mission inputs, executing nominal mission functions and producing mission outputs according to the typical mission rhythm, timelines and sequences resulting in end-user goals (products, services, and timeliness)*
- **Mission Critical Event**
  - *Events that contribute to the overall success of the mission Critical Events can consist of any of the following types of events that are necessary for a successful mission: first time events, critical reoccurring event (i.e., daily nominal operations), and critical situations (i.e., transitions between events).*
- **Critical Mission Contributors**
  - *All items (hardware and software) and conditions (initial conditions, dependencies/pre-requisites, sequence, timing, interactions) that have failure consequences leading to end of mission or severe mission degradation*

TLYF Process Flow

Mission and Fault-Informed Paths



Mission and Fault-Informed Paths

TLYF Distinctions

Mission-informed

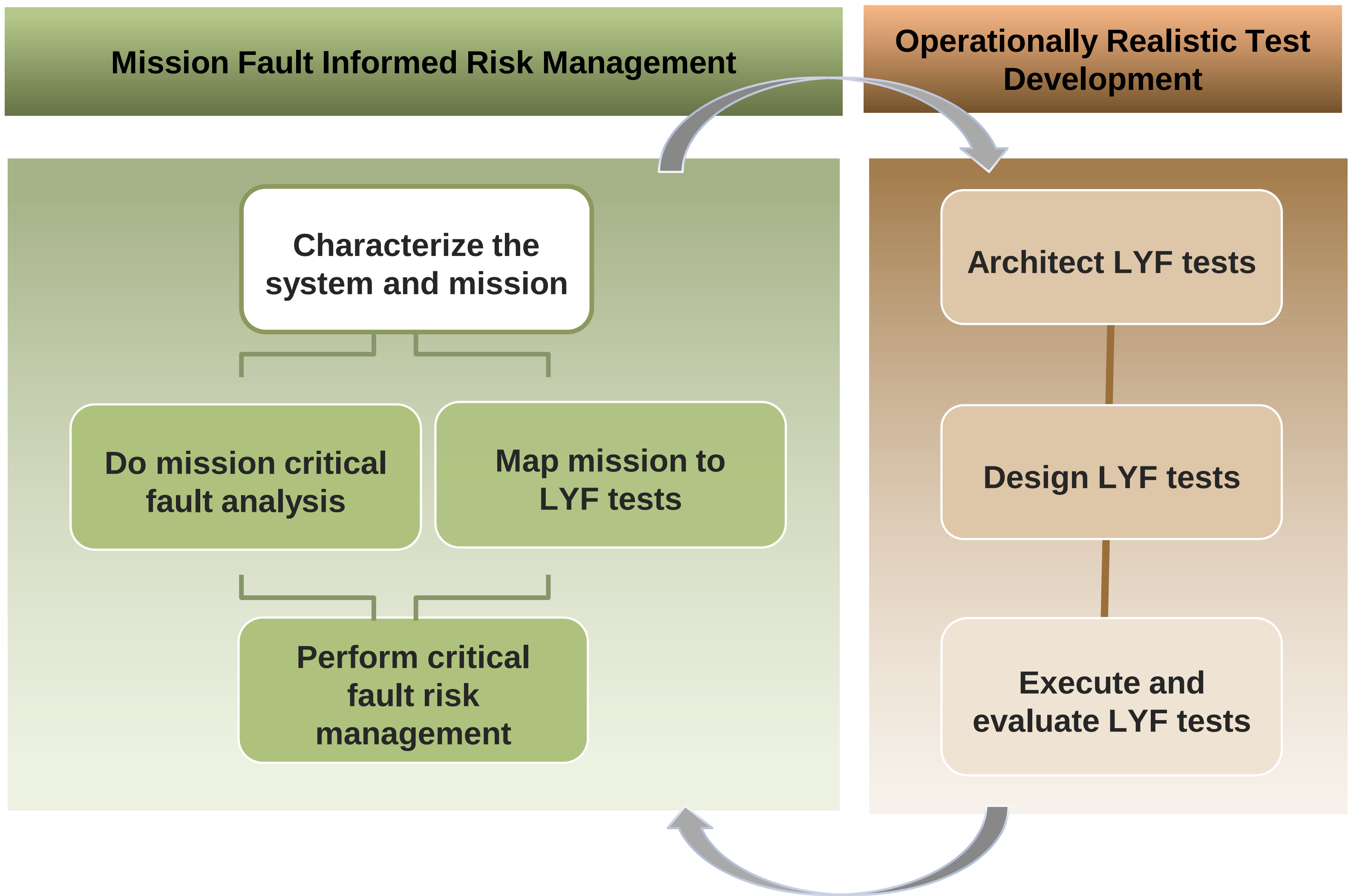
- Mission timeline, critical events, transitions, and critical mission contributors
- Pyramid Application
- Mission Critical Event & Contributors Coverage
- LYF Test Exceptions Identification
- Operationally realistic tests that address mission critical events and contributors

Fault-informed

- Mission timeline, critical events, transitions, contributors and mission-ending failure situations with paths and contributors to failure
- Pyramid Application
- Mission-Critical Event & Contributors and Failure Situations & Contributors Coverage
- LYF Test Exceptions Identification and Criticality Evaluation
- Operationally realistic tests that address mission critical events, potential mission-critical flaw paths and contributors

TLYF Process

Characterize the System and Mission



Lessons from the Mars Program

Two Failed Missions Failure Review Board Findings*

Mars Climate Orbiter
Sept 1999

Mars Polar
Lander
Dec 1999

Courtesy of NASA/JPL-Caltech

- …**future projects must review their operational scenarios and mission timelines for consistency with their Mission Plans**
- **Recommendation: increase the amount of formal and informal face-to-face communications with all team elements,… especially for those elements that have critical interfaces**

** Beutelschies, "That One's Gotta Work"* IEEE, 2001.*

This is a team sport!

Characterize the System and Mission

System Aspects

- Design
- Architecture
- Functional Flows
- Interfaces
- Technology Upgrades
- Manufacturing Processes/Vendors

Mission Aspects

- Primary Mission Success
- Mission Products/ Services
- Concept of Operations
- Mission Phases / Events /Timelines / Sequences
- States, Modes, & Transitions
- Operations Interactions
- Design Reference Mission

Program Resources

- Support Systems
- Legacy / Heritage Systems
- Acquisition Scope
- Tasker Requirements
- End User Needs

Characterize the System and Mission

Description

- Develop an understanding of
  - *the system,*
  - *its mission,*
  - *its core phases and associated events and/or activities,*
  - *how the mission will be successfully executed*

- System Aspects

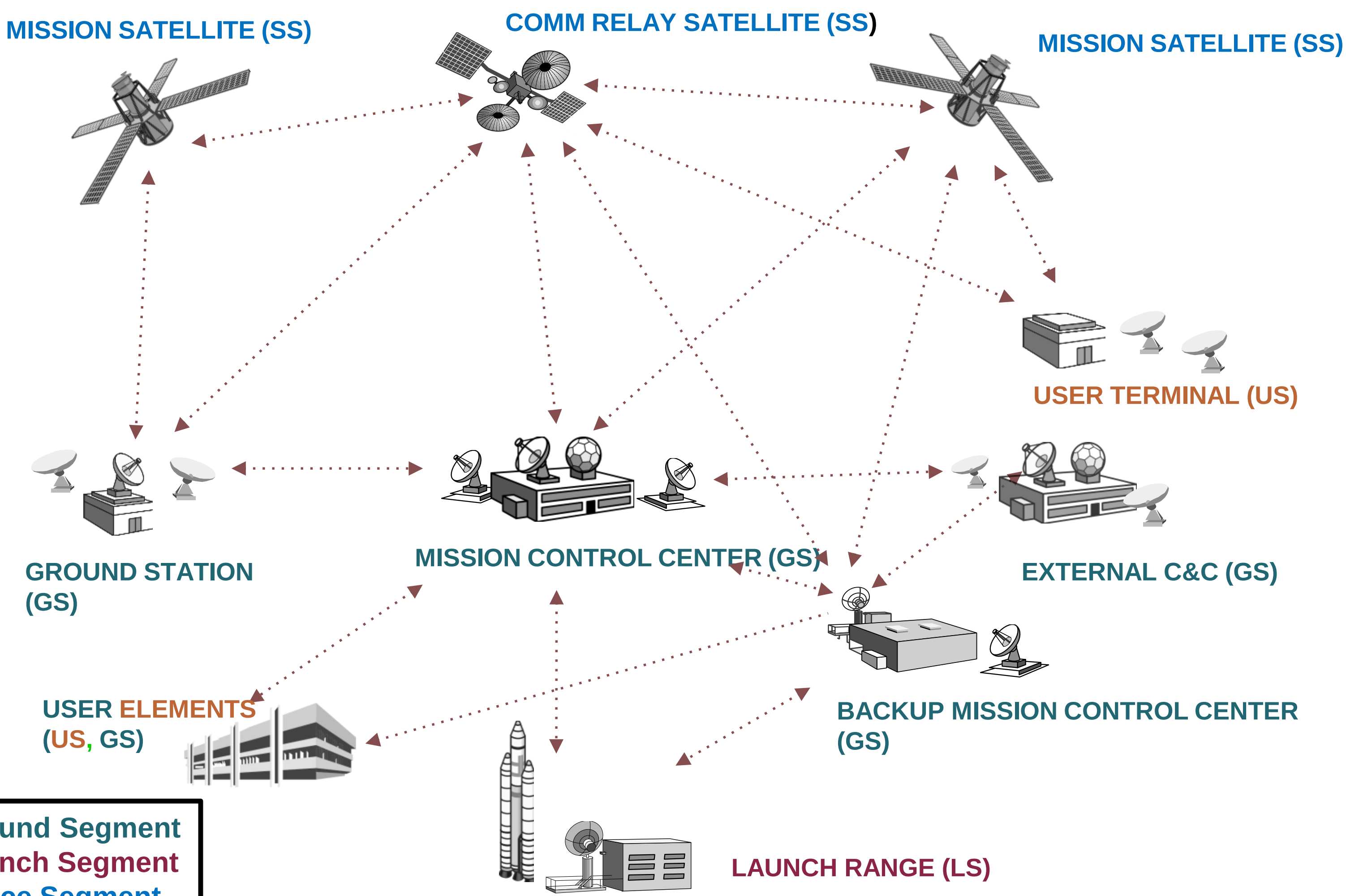
- Mission Aspects

- **Mission characteristics** provide a mechanism for identifying the attributes for conducting a mission

You can't Test Like You Fly if you don't know How, What and When you're flying

Notional Operational Space System

May Involve Many Elements



GS	Ground Segment
LS	Launch Segment
SS	Space Segment
US	User Segment

Search & Rescue High Level Operational View

Image from NOAA.gov

Role of Satellites and Control Centers in SAR

REFERENCE

1. ELTs, EPIRBs, and PLBs operate on the 406 MHz frequency.
   a. *Each 406 MHz beacon transmits a unique digital code that identifies the type of beacon and that allows registration data to be associated with the beacon.*
   b. *The registration data provides information such as the beacon owner; the type of platform the beacon is associated with; emergency points of contact; and much more.*
2. After the satellite receives a beacon signal, it relays the signal to earth stations referred to as local user terminals (LUT).
3. The LUT processes the data, computes the location of the distress beacon, and transmits an alert message to its respective Mission Control Center (MCC) via a data communication network.
4. The MCC performs matching and merging of alert messages with other received messages, geographically sorts the data, and transmits a distress message to another MCC, an appropriate SAR authority such as a national Rescue Coordination Center (RCC) or a foreign SAR Point of Contact (SPOC).
5. The RCC investigates the beacon alert and launches assets to find the parties in distress when necessary.

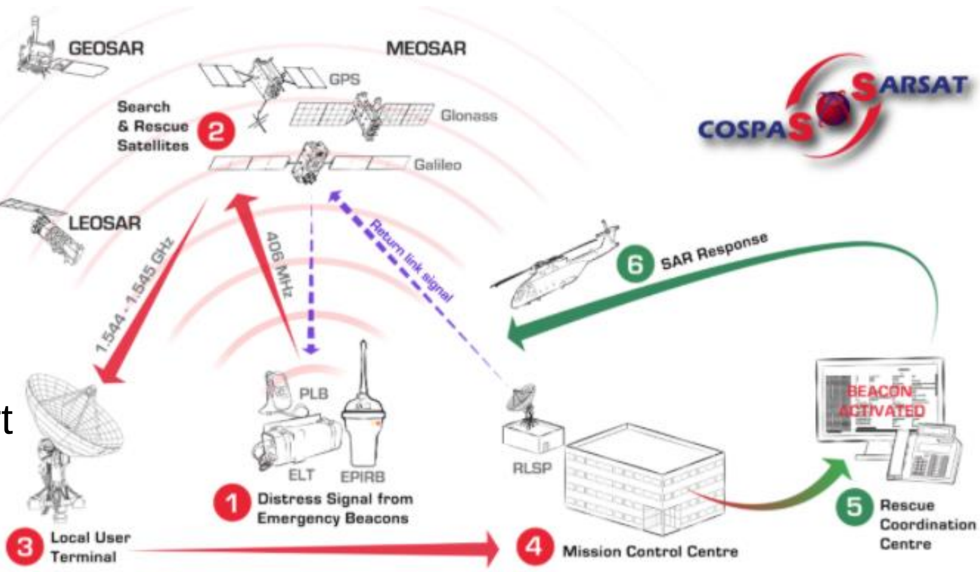


Image from NOAA.gov

State Search and Rescue System Refresh

- **Coming up on state's 150 anniversary of statehood**
  - *State has many natural attractions including mountains and lakes*
  - *Encouraging tourists to come celebrate any time of the year by hiking, skiing, boating, hang gliding, off-roading, rafting and similar activities*

- **New state office established to integrate search and rescue efforts**
  - *Update and integrate essential systems to take advantage new NOAA / NASA SAR satellite capabilities*
  - *Update existing state and SAR communications assets & incorporate 5G*
  - *Acquire new, lightweight, improved signal user beacons to distribute to tourists at main attractions*
  - *Provide common test and training opportunities to integrate local SAR assets*

Search and Rescue Concepts of Operations

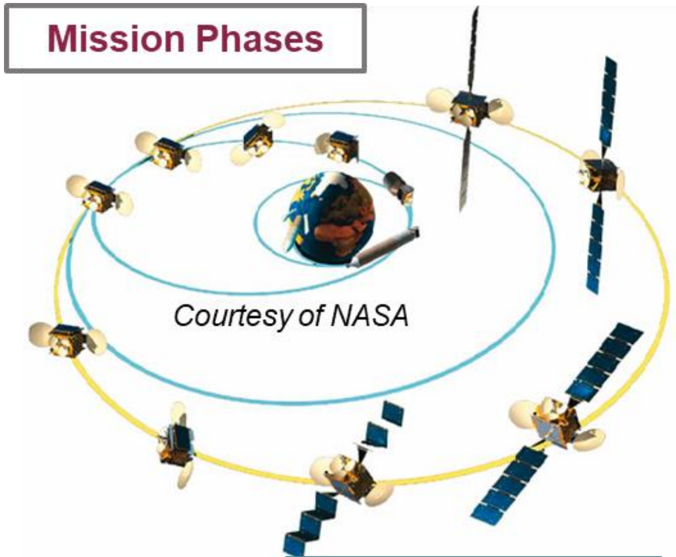
- **Search and Rescue manages and coordinates the response of local non-Urban Search and Rescue (USAR) resources in response to any incident involving search and rescue operations. These include, but are not limited to,**
  - *Mountain, lake, river, off-road and woodlands incidents*
  - *Incorporates new emergency SAR capabilities into established emergency service and search and rescue procedures*
  - *Responsible for situation assessment and determination of resource needs*
  - *Coordinates with local incident commanders to summon additional resources*

- **PROCEDURES**
  1. *The State SAR Coordinator is responsible for coordinating SAR resources and operations within the State.*
  2. *Coordination with all supporting and other appropriate departments, agencies, and organizations will be performed to ensure continual operational readiness.*
  3. *Applicable plans for appropriate use of personnel and equipment tasked for SAR missions will be activated upon initial coordination of rescue mission.*

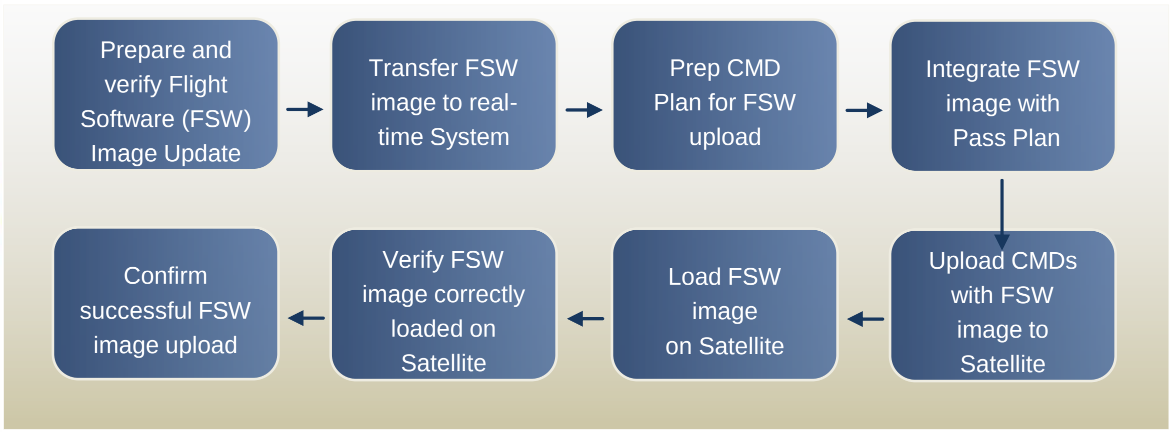
Representation of Operational Activities

Examples of Mission Phases/Threads/Timelines/Scenarios

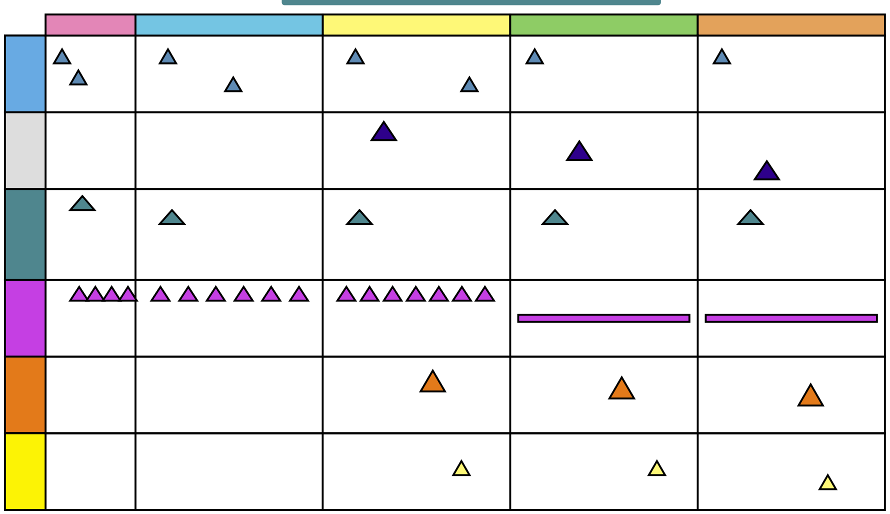
Mission Phases



System Thread: Flight Software Upload



Mission Timeline



Mission Scenario

- **Earth stare**
- **Detect missile launch**
- **Acquire & store images**
- **Acquire & store spectra**
- **Report acquisition**
- **Report trajectory**
- **Transmit images**
- **Transmit spectra**
- **Return to earth stare**

Mission Thread Example

Example for Search

- The USMCC matches beacon signals to identify those coming from the same source and merges them to improve position accuracy.
  - *Registration information is then appended to the 406 MHz beacon distress alerts that are registered in the U.S.*
  - *The location of the alert is geographically sorted and the data is distributed to the appropriate recipient*
- Thread actors/components: SARSat, USMCC, State SAR control center
- Thread trigger: distress beacon signal

Listening

Acquisition sensor detects a signal

Signal sent to USMCC

Location determined and send to State SAR CC

State SAR CC routes notice to appropriate local assets

USMCC – United States Mission Control Center

Mission Characteristic Classes for Space Missions

- **Mission characteristics provide a mechanism for identifying the attributes for conducting a mission**
  - *They include all aspects for mission operations/execution in terms of components, conditions, interfaces,* ***transitions, transactions****, processes, and environments.*
  - *There is often* ***concurrency*** *amongst these characteristics which will prove important when designing/evaluating LYF tests.*

- **Characteristic classes may include:**
  - *End-to-end (integration or hierarchy) level*
  - *Configuration*
  - *Time & Timeline*
  - *Uplink (commands)*
  - *Downlink (state of health, mission data)*
  - *Environments (internal, ascent, space, ground)*
  - *Mission Planning & Operations*
  - *Products/Outputs/Services*

You'll need to come up with characteristic classes appropriate for your mission area

Mission Characteristic Classes for Search & Rescue

Which of these apply to SAR?

Exercise

- **End-to-end (integration or hierarchy) level**
- **Configuration**
- **Time & Timeline**
- **Uplink (commands)**
- **Downlink (state of health, mission data)**
- **Environments (internal, ascent, space, ground)**
- **Mission Planning & Operations**
- **Products/Outputs/Services**
- **Others?**

Q

Mission & System Characterization

Exercise #1: What's this all about?

Search and Rescue (SAR) Exercises

- **All exercises will be done as a solo effort**

- **Pick your role**
  - *Systems Engineer*
  - *Chief Tester*

- **Pick your organization (something close to your real world organization)**
  - *State SAR Office*
  - *SAR satellite contractor*
  - *SAR user equipment contractor / manufacturer*
  - *Communications equipment contractor*
  - *Mission control center contractor*
  - *Search equipment (helicopter, aircraft, or rescue boat contractor)*
  - *Rescue equipment contractor*
  - *Other (specify in chat line)*

Search & Rescue High Level Operational View

Image from NOAA.gov

Critical Events and Mission Contributors

- **Critical Events -** can consist of any of the following types of events that are necessary for a successful mission:
  - *first time events,*
  - *critical reoccurring events (i.e., daily nominal operations), and*
  - *critical situations (i.e., transitions between events).*

- **Critical Mission Contributors -** All items (hardware and software) and conditions (initial conditions, dependencies/pre-requisites, sequence, timing, interactions) that have failure consequences leading to end of mission or severe mission degradation

Search & Rescue Mission & System

Mission Objective: Rescue people in distress in a timely manner

Mission Phases

- **Notify (HELP!!!)**
- **Detect**
- **Respond (Let appropriate organizations know)**
- **Search**
- **Rescue (THANK YOU!)**

System Elements

- **Using the Operational View, identify the system elements associated with each mission phase:**
- **PHASE** ______________________
- **SYSTEM ELEMENTS**
  1. _______________
  2. _______________
  3. _______________
  4. _______________

Exercise

Search & Rescue Mission & System

What are Critical Events and Contributors?

- **Critical Events** per mission phase
- Example: Mission Phase DETECT
  - *Receipt of User distress signal on satellite*
  - *Transmission of distress signal information to USMCC*

- **Mission Contributors** per mission phase
- Example: Mission Phase DETECT
  - *# of concurrent distress signals*
  - *Space weather event*
  - *Health of on-board receiver*

- Notify (HELP!!!)
- Detect
- Respond
  - *Communicate*
  - *Search*
  - *Rescue*

Mission Phases

- Users (Hikers, Boaters, Off Roaders, Rafters)
- Communication Assets
- Detection Assets
- Responder Assets

System Elements

Characterizing the Mission

Fill in at least one row

Primary mission success criteria: ______________________________

____

Mission phase success criteria: ______________________________

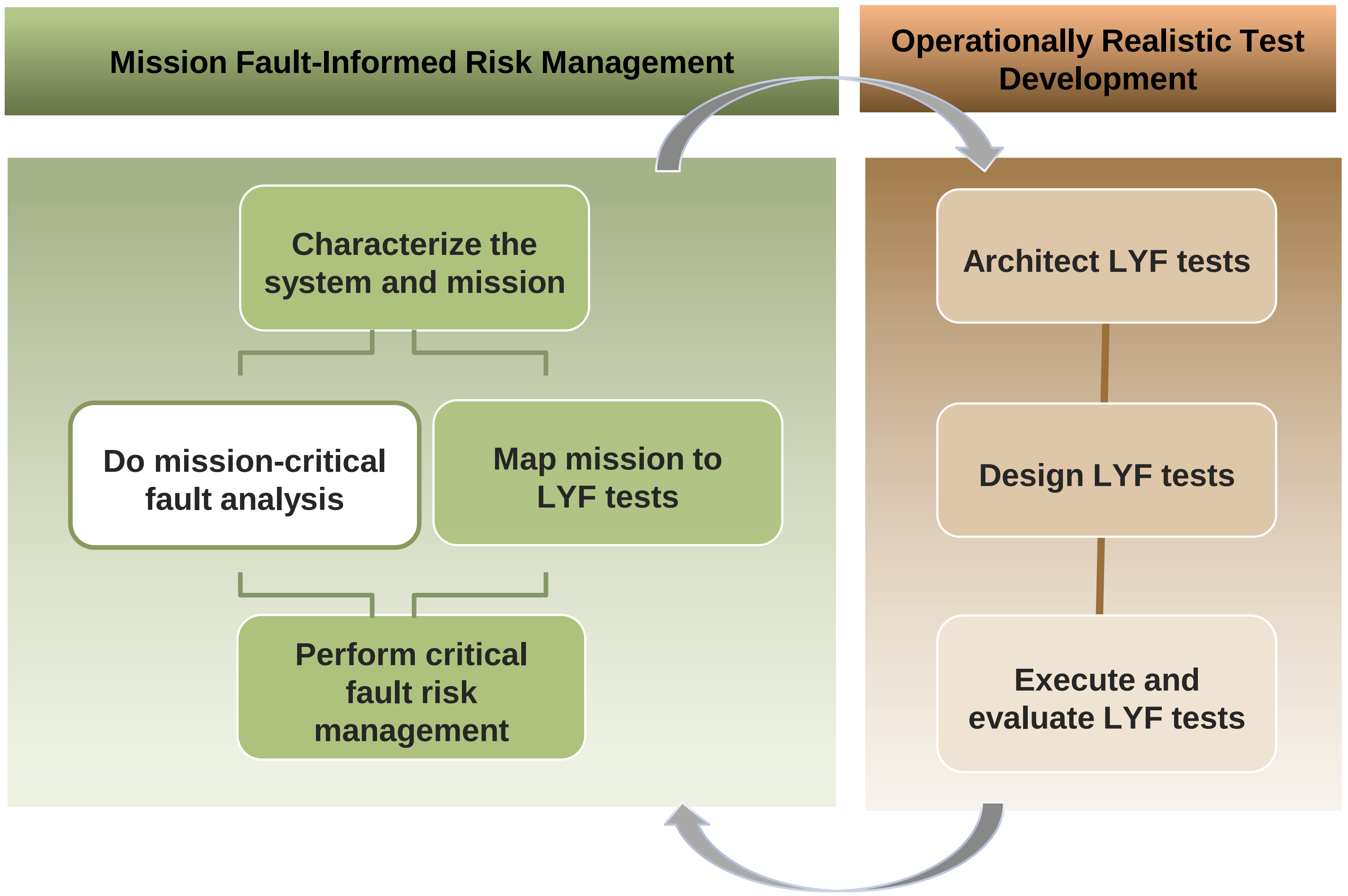
____

Mission Phase	Mission Critical Event	Mission Phase Objective	End-to-End Configuration	Critical Mission Contributors

Exercise

TLYF Process – Fault-informed Path

Do Mission-Critical Fault Analysis



Lessons from the Mars Program

Two Failed Missions Failure Review Board Findings*

Mars Climate Orbiter
Sept 1999

Mars Polar
Lander
Dec 1999

Courtesy of NASA/JPL-Caltech

- **Recommend… a systematic assessment of all potential failure modes**
- **Recommendation: Utilize established risk management tools such as fault-tree analysis and FMECA**
- **Odyssey implementation: Test Like You Fly**
  - *Once faults were identified and collected into a list, detail how the fault mitigation would be verified*
  - *Verification would be assessed for "are you testing like you are flying" to ensure that the test realistically simulated the event.*
  - *The fault tree provides input to LYF test exceptions*

** Beutelschies, "That One's Gotta Work"* IEEE, 2001.*

FMECA – Failure Modes, Effects, and Criticality Assessment

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 of NASA/JPL-Caltech

Mars Odyssey February 2002

Successful Mission!

Do Mission Critical Fault Analysis

Description

Also known as a pre-mortem

- **Definition: a pre-launch analysis that examines a system's operational timeline (discrete critical events and transitions) and focuses on what could go wrong with the mission (i.e., mission-ending failures)**

Applying TLYF Lens

- **Unlike other failure analyses it starts from the top with the mission failures**
  - *It uses the system's operational timeline to identify mission-critical events and transitions*
- **It determines the flaws that could prevent success for each mission objectives**

*Process for Mission-Critical Fault Analysis**

Initial Activities and Longer Term Activities

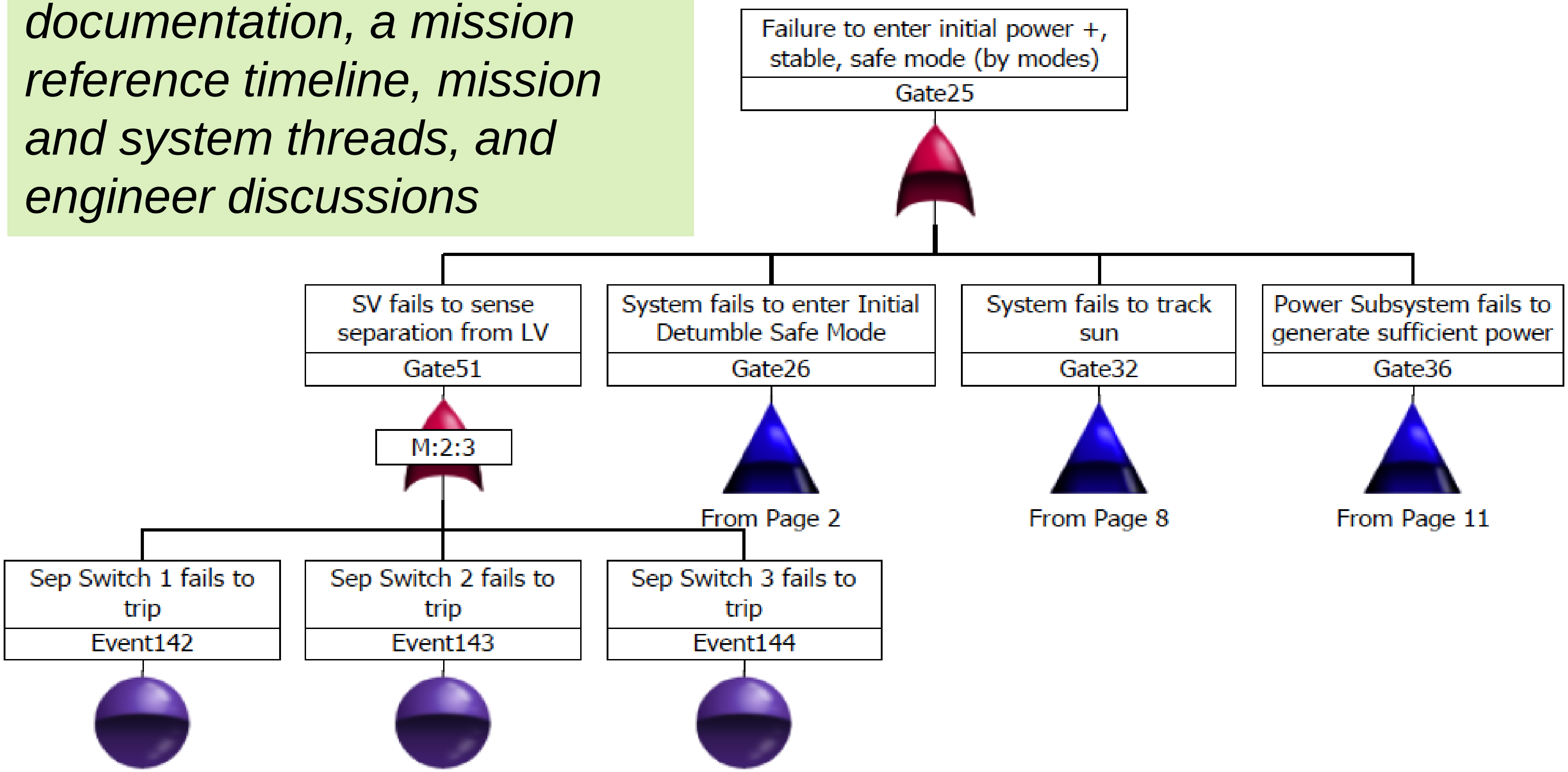
- Assemble the Team: Include a Facilitator
- Establish a Schedule and Expected Outcomes
- Conduct the Failure Investigation Prior to Launch/Mission Execution
  - *Identify critical events and mission characteristics.*
  - *Identify mission-critical situations—potential mission-ending failures*
  - *Identify potential contributors.*
- Identify Critical Fault Path Exoneration Methods
  - *Once fault trees or fishbone diagrams are defined, it can be determined what kind of evaluation or method is necessary to exonerate branches or bones (flaws).*
  - *If mitigation is not possible, add the risk to the program's formal risk management process*

***** Beutelschies, Guy, "That One's Gotta Work: Mars Odyssey's Use of a Fault Tree Driven Risk Assessment Process," IEEE, 2001.***

Design Premortems, Fault Informed Risk Management

Autonomous Spacecraft Initialization Failure Fault Tree

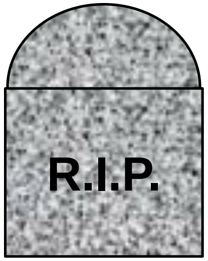
Sample fault tree derived from satellite program design documentation, a mission reference timeline, mission and system threads, and engineer discussions



There are ready made tools to assist with fault tree products

Mission Critical Fault Analysis

Exercise #2: What could possibly go hideously wrong?



First-Time and Mission-Critical Events

Exercise: Mission Failure & What Can Go Wrong

SAR Timeline

Timeline	Critical Event
Readiness Baseline	Validation of State SAR Readiness
T + 0	Person in distress activates beacon
T + a few seconds	Satellite receives and transmits distress to LUTs
T + 2 minutes	LUT makes position calculation and transmits to an MCC
T + 5 min	MCC identifies and contacts appropriate search and rescue POCs
T + ??	SAR resource personnel determine initial response
T + ???	Search resources deployed; rescue resources arranged
T + ????	SAR response agencies caucus to determine if additional resources needed

Phase transition

- **Mission Failure: People not rescued in time**
- **What Can Go Wrong?**
- **What are Some Critical Mission Characteristics?**
- **How?**

Exercise

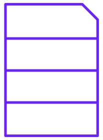
Pre-Mortem: <u>Mission</u> Failures

The bad news

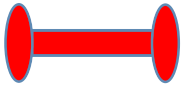
Mission Failure	Mission Phase	Notes

- **We will have a 3-minute timed self-brainstorming session**
  - *Write down as many* ***mission*** *failures as you can in the time allotted*
    - Keep it at the mission level, including mission phase transitions
    - Mission failures can reflect failures of the segment you identify with
  - *Each person then reports one failure and identifies the applicable mission phase on the chat line*

- **We'll use some of the results from this in later process steps**

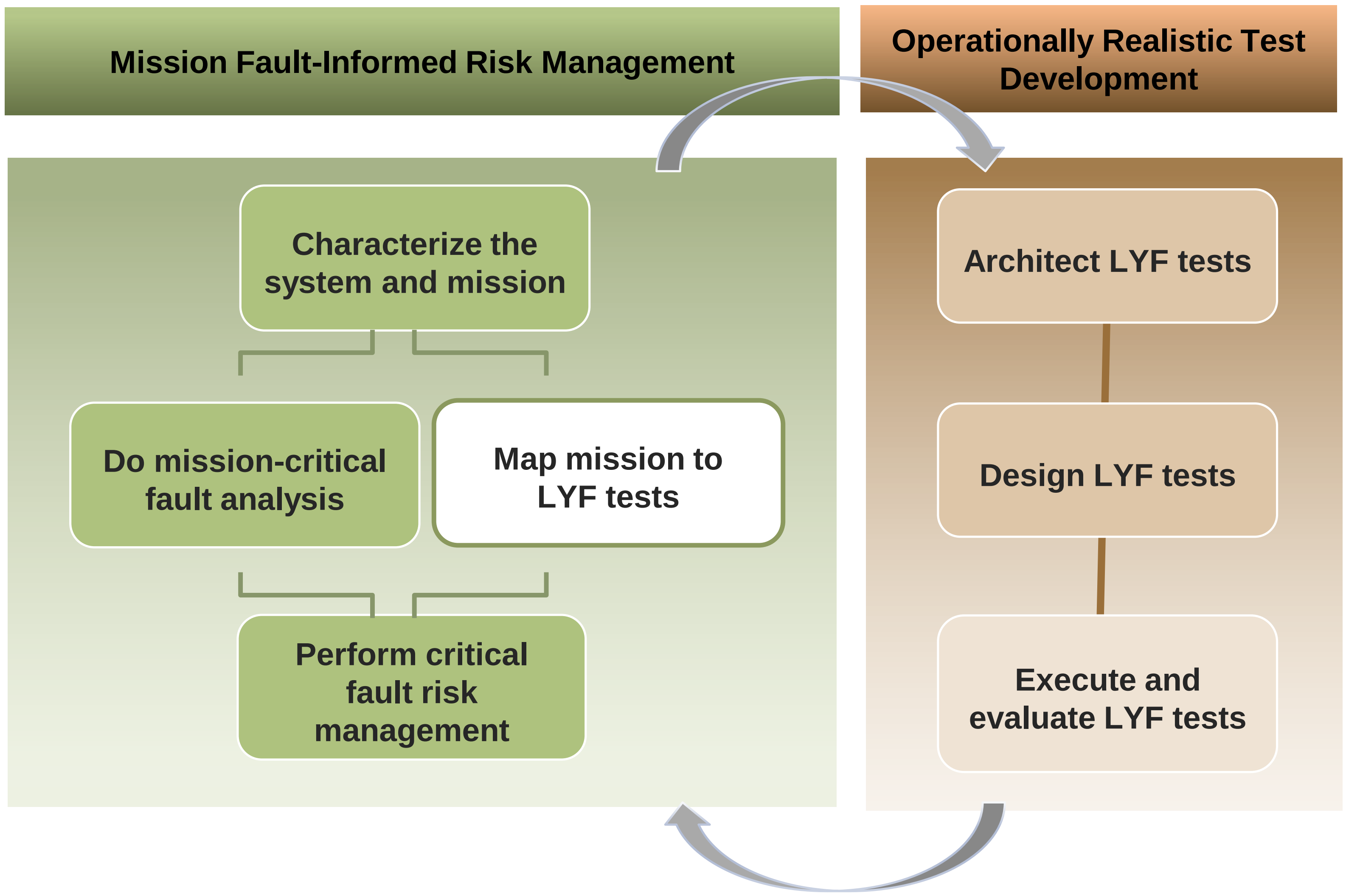


Exercise



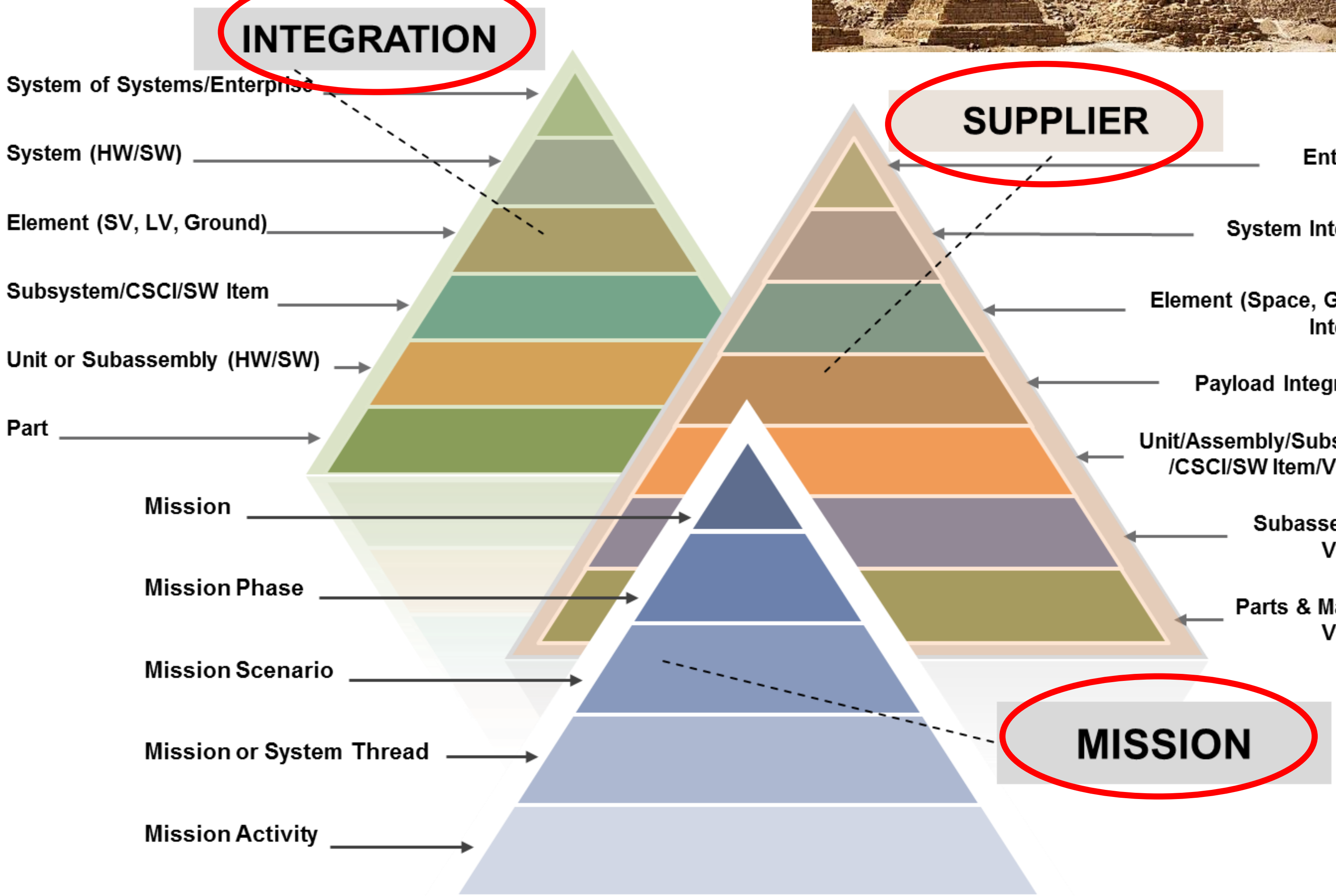
TLYF Process

Map Mission to LYF Tests



TLYF Pyramids

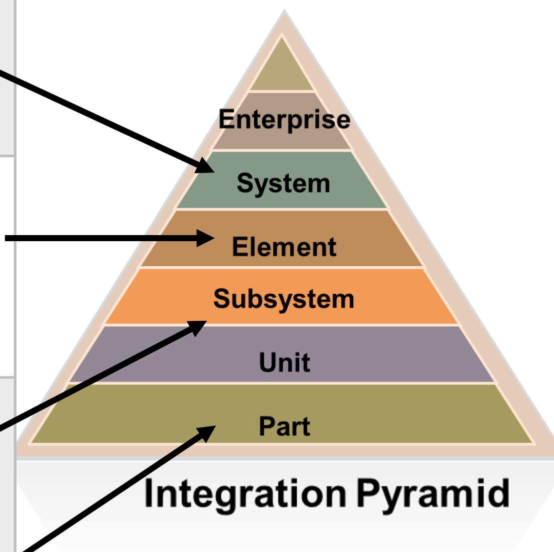
Allocating Operationally Realistic Tests



Failing to Test Like You Fly

Along the System Integration Pyramid

Vehicle	Mission-Critical Anomaly & Root Cause	Integration Level of Flaw Detectability
Titan CT-2	*Failure to separate SV.* Miswire/numbering error for single payload	Integrated LV & SV
Ariane V	*Primary and secondary processor shutdown due to velocity overflow*. Inertial Reference System disabled. "Dead code" inherited from Ariane IV	Integrated Flight SW & Control Subsystem
ESEX Arcjet	*Battery explosion.* "Heritage" battery & charging system not able to sustain unique charging scheme	Payload Power Subsystem
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	Valve Assembly



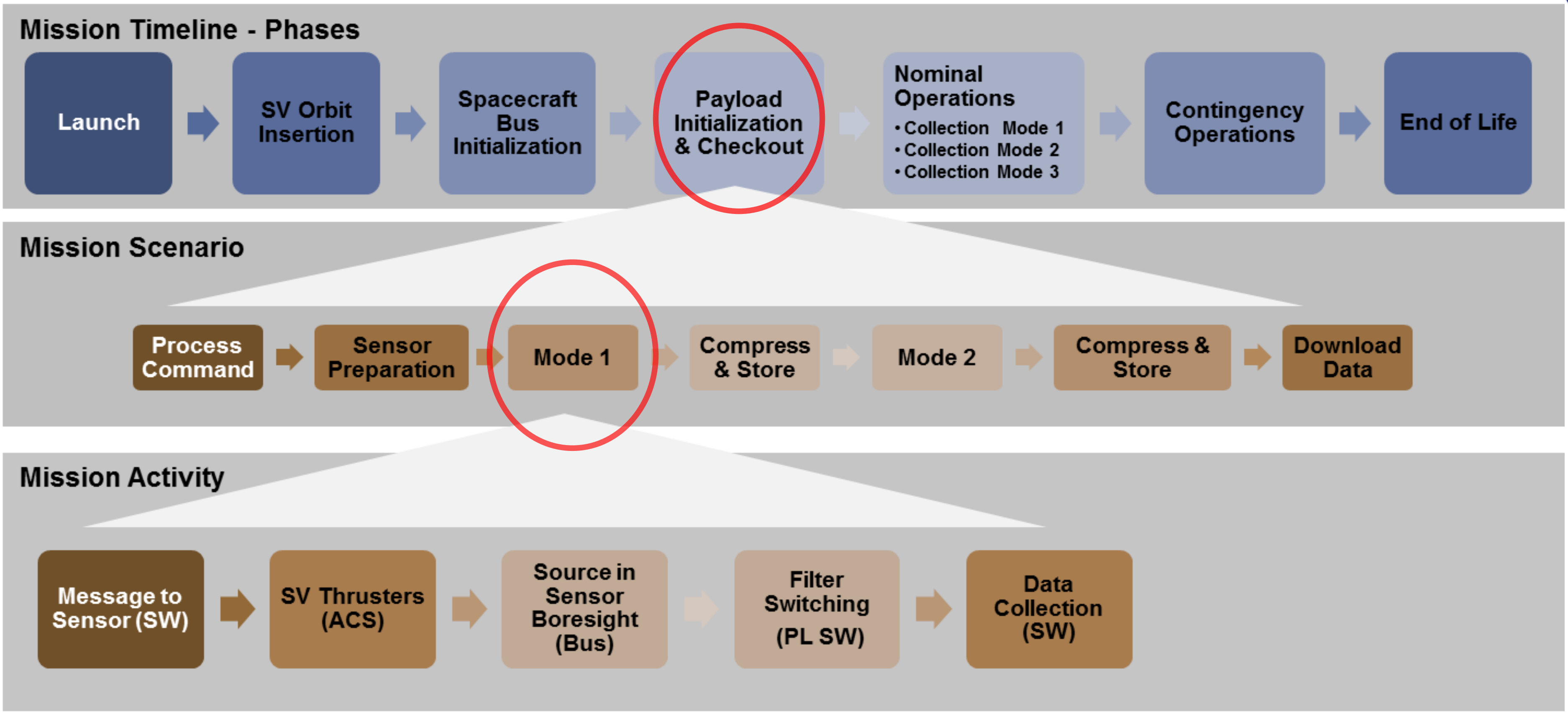
Flaws can be introduced at any level of integration and it's best to catch them there

LV Launch Vehicle

Notional Mission Decomposition

Payload System Activities

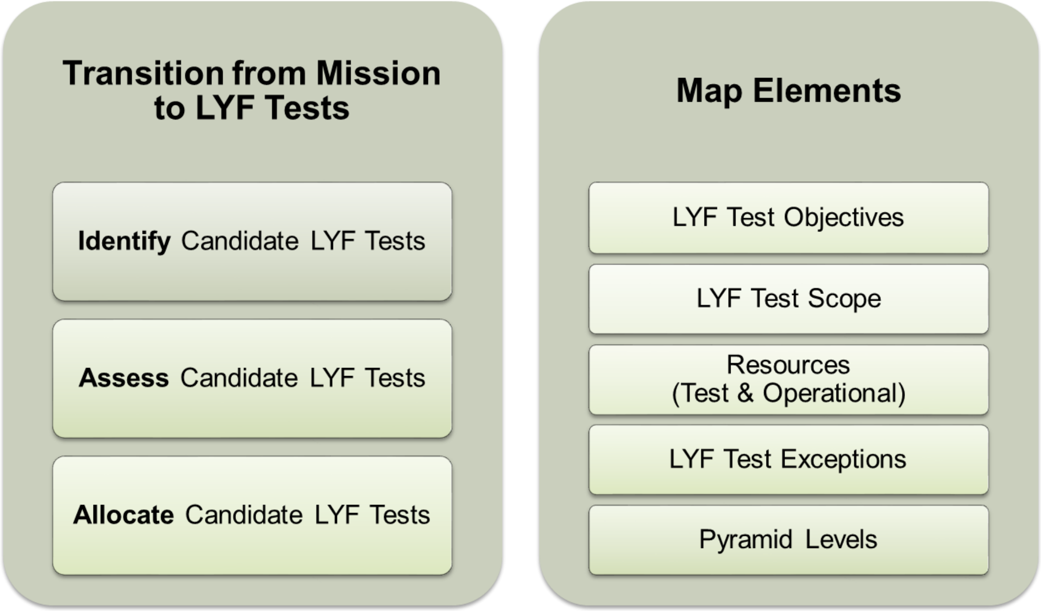
What does decomposition look like for your project?



Map Mission to LYF Tests

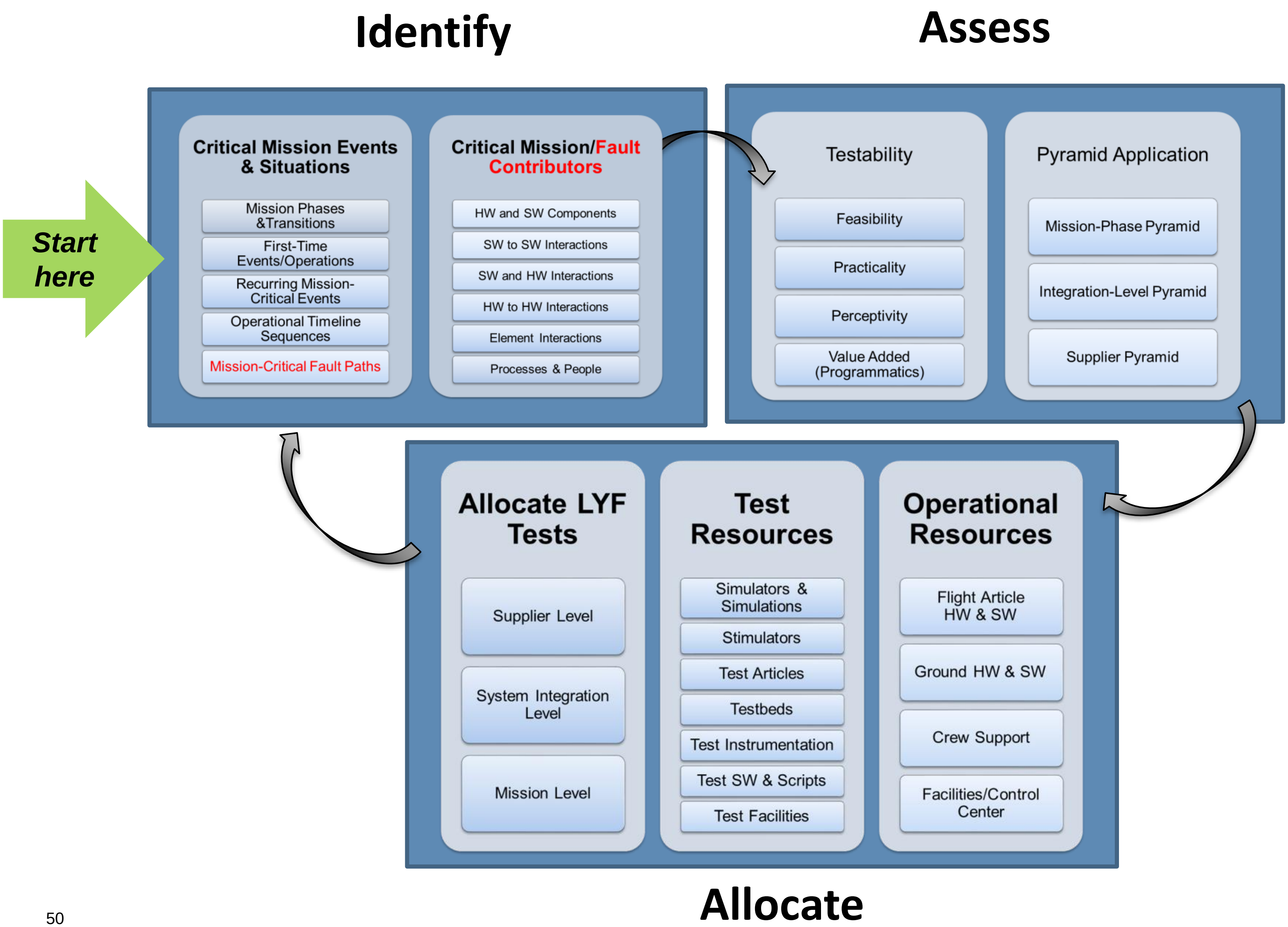
Description

- Map Mission to LYF Tests contains three key LYF test building activities
- **Identify** Candidate LYF Tests based on the mission
- **Assess** Candidate LYF Tests for testability
- **Allocate** LYF Tests into program test plan



Start with the Mission, then formulate the tests

Map Mission to LYF Tests



Mapping the Mission to Tests

Resulting Products

For each allocated LYF test, the following is generated:

Mission-informed Path

- **Test objective based on corresponding mission objective**
- **Mission Critical Event(s) test coverage**
- **Allocate to Pyramid level(s): supplier, system integration, & mission**
- **Allocate operational and test resources for test**
- **Begin LYF test exceptions list (high level)**

Fault-informed Path

- ***Mission-informed Path products* +**
- **LYF test exceptions list (high level) – criticality rating based on Fault Trees**
- **Mission-ending Failure Situation(s) and Contributors test Coverage**

Poll: What distinguishes LYF Testing from other types of tests?
Select the best answer:

a. Flight items are used in the test
b. An environment similar to the operational environment is created for the test
c. The mission is used as the starting point for building test objectives
d. Real ground operators are used for testing

Q

Using System Thread End-to-End Configurations to Identify LYF Tests

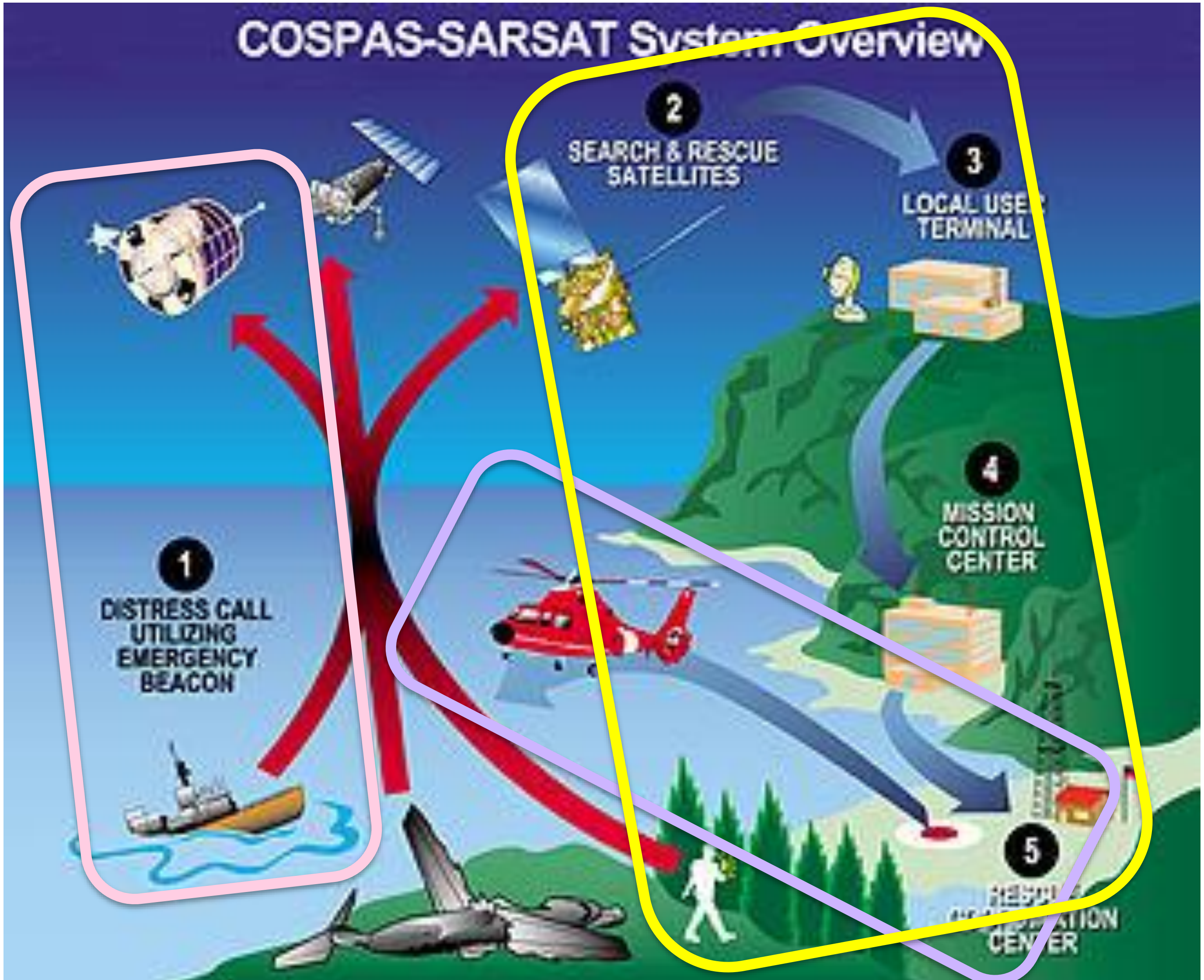
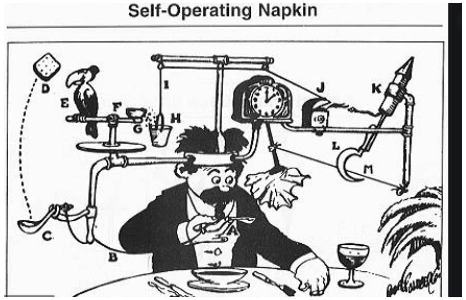


Image from NOAA.gov

Testability

Assessing the Testability of Each Candidate LYF Test

- **The testability assessment is based on four factors:**
  - ***Feasibility***
    - Could it be done?
  - ***Practicality***
    - Shouldn't need Rube Goldberg design
  - ***Perceptivity***
    - Sensitive to the parameters being measured for the test success criteria, or is sensitive to particular flaws being explored
  - ***Programmatic value***
    - Evaluated in terms of its required resource needs and constraints (e.g., money, time, personnel, and equipment) versus the risks of not allocating those resources for a test



- **The testability assessment can change as a result of the pyramid level under consideration**

Mapping Mission to Test

Exercise #3: Let's do this!

Process to Assist with Identifying Candidate Tests

- Examine mission architecture, CONOPS, timelines
- Look at notional mission phases
- Identify phase transitions, sequences, handoffs, concurrent activities
- What mission-critical and first-time events are included?
- How much of each mission phase has been/will be tested?
- Are there any critical events that need to be tested in an operationally realistic manner under several conditions or scenarios?
  - *Seasonal?*
  - *Process testing?*
  - *Testing for time?*
- What mission events / activities should your list of candidate LYF tests include?
- What critical mission characteristics would you want present in a LYF test?

Keep the focus on mission execution

Exercise

Candidate Operationally Realistic Tests

Candidate Test	Mission Objective	Test Objective	~ Test Duration	Key Characteristics	LYF Test Exceptions

Using one of the techniques identified in previous material, identify at least one candidate test and as many attributes as possible in the table.

If you are taking this session with colleagues, feel free to collaborate offline.

These will be used later in the process

Exercise

Testability Assessment for Candidate LYF Tests

Evaluate previously identified candidate tests

Testability	Operationally Realistic LYF Test Options		
Test ID			
Test Resource			
Feasible?			
Aspect of Mission Validated			
Practical?			
Perceptive?			
Value Added?			

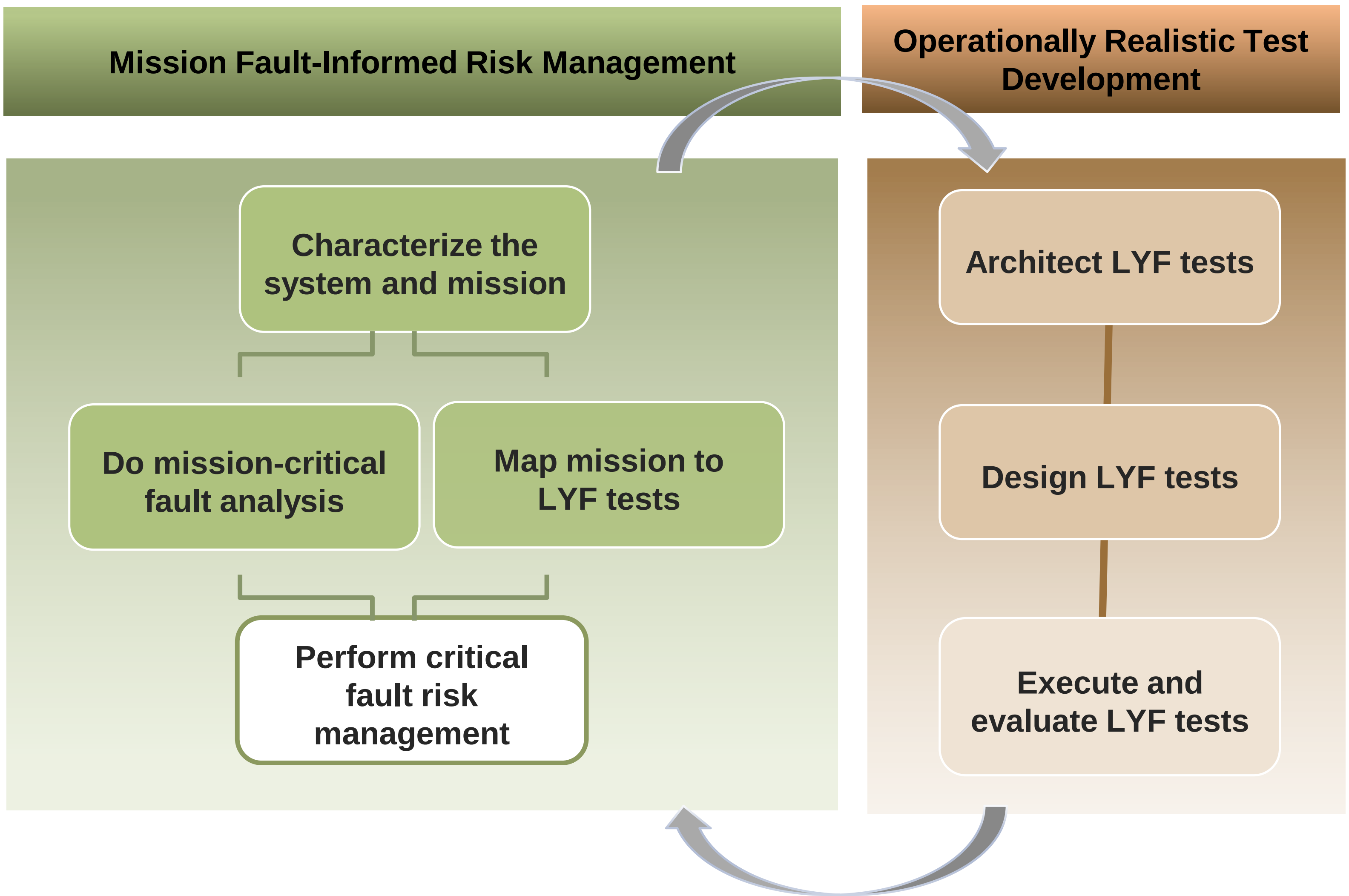
Do a testability analysis on at least one candidate test and note as many evaluations as possible in the table.

If you are taking this session with colleagues, feel free to collaborate offline.

Exercise

TLYF Process

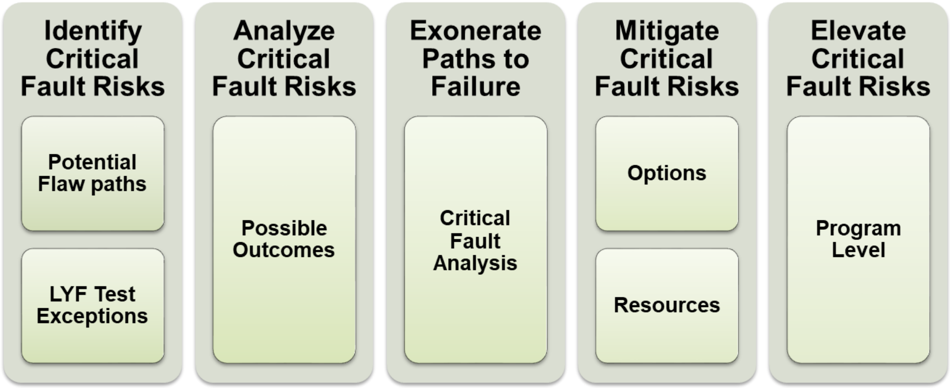
Perform Critical Fault Risk Management



Perform Critical Fault Risk Management

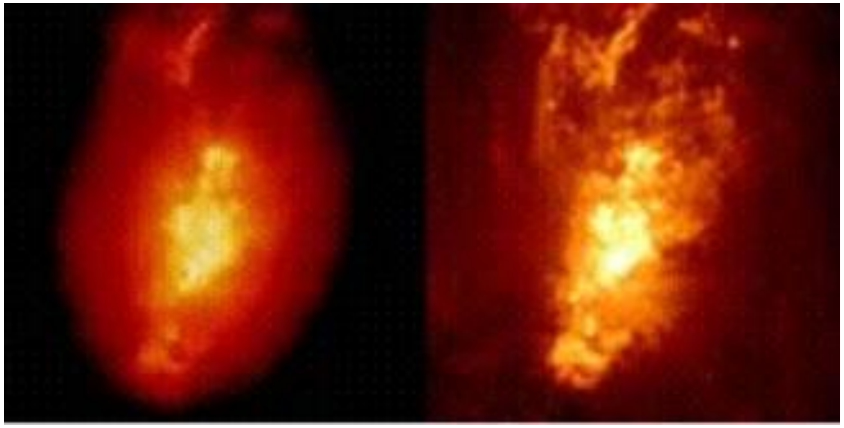
Description

- **Encompasses identification, analysis, mitigation planning and implementation, monitoring, and elevation of Critical Fault (CF)-related risks**
- **Identify mission-critical risks based on:**
  - *Potential flaw paths to mission-critical failure situations, as an output of the mission-critical fault analysis*
  - *LYF test exceptions identified during the LYF test design process*
- **Perform mission-critical fault analysis for identified LYF test exceptions**
  - *Is there a critical flaw that could be missed?*
- **Exoneration plan for each potential path to failure, or provide evidence of the nature of the discovered (actual) flaw**
- **Mitigate discovered flaws**
- **Elevate CF-related risks that cannot be exonerated within allocated resources**



Lessons from Hubble Space Telescope

Everything You Wanted to Learn about TLYF



Courtesy of NASA/Space Telescope Science Institute (STScI)

Before *After*

- **Lesson:** Conduct end-to-end tests of integrated equipment
- **Lesson:** Critical fault-related risks that cannot be exonerated should be identified and elevated

Courtesy of NASA/Space Telescope Science Institute (STScI)

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."

Initial Severe Degradation to Mission

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

Critical Fault Risk Management

Resulting Products

- **Critical Faults, Critical Events, and Contributors:**
  - *Exoneration plan for each failure path identified in MCFA (I, A, D, & T)*
  - *Exoneration methods for each failure situation (includes successful completion of first time / mission critical events) (I, A, D, & T)*

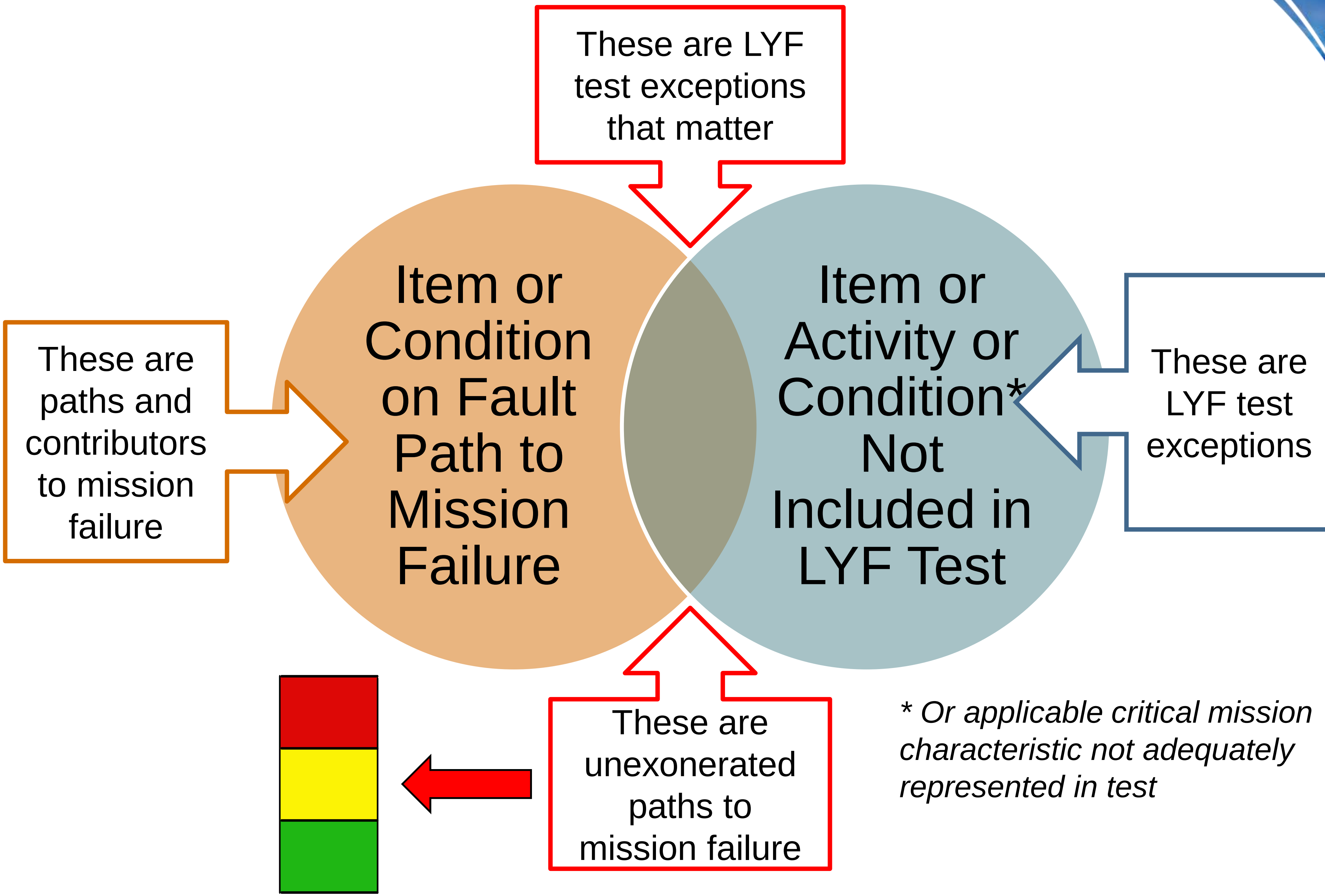
- **TLYF associated program risks:**
  - *List of first time / mission critical events with no planned validation*
  - *List of MCFA failure paths and contributors not addressed in test*

- **LYF test exception handling**
  - *List of LYF test exceptions linked to MCFA branches*
  - *LYF test exception risk evaluation and assessment (MCFA)*

- **Risk mitigation plans**
  - *Proposed new LYF test candidates (if applicable)*
  - *Updates to current LYF tests (replace test resource with operational source)*

I = Inspection; A = Analysis; D = Demonstration; T = Test

FIRM and LYF Test Exceptions



** Or applicable critical mission characteristic not adequately represented in test*

Lessons from the Mars Program

*Two Failed Missions**

Mars Climate Orbiter
Sept 1999

Mars Polar Lander
Dec 1999

Courtesy of NASA/JPL-Caltech

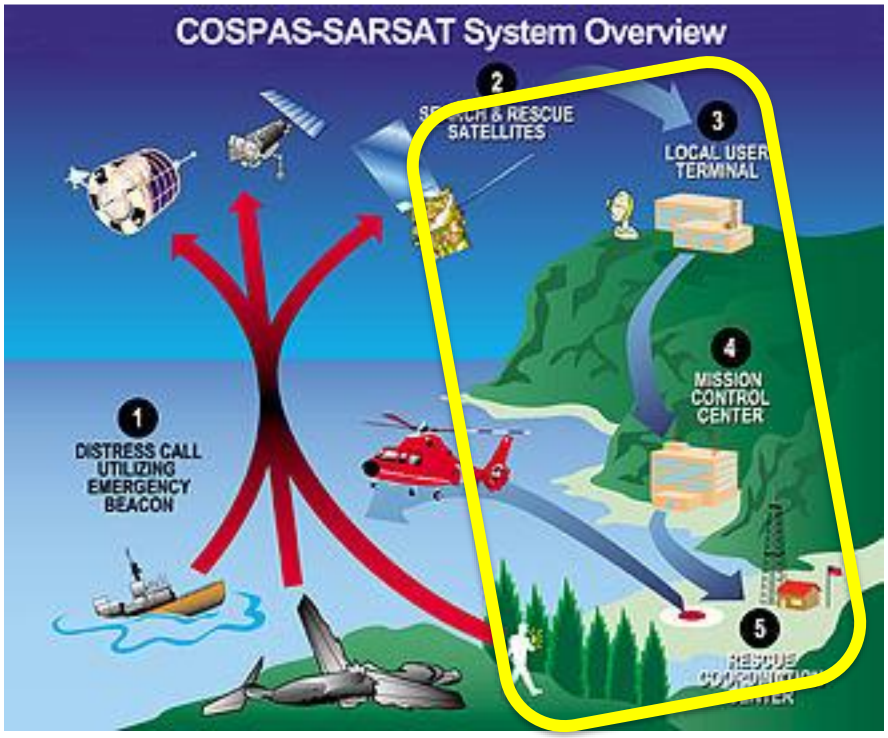
- **Failure review board findings**
  - ***Project-level decisions affecting*** *requirements, schedule, resources, and* ***risk*** *should be made with full representation by all project elements with expertise relevant to the decision issue*
    - …future projects must review their operational scenarios and mission timelines ... to determine that the necessary planning is in place **to support their risk management strategies**
  - *Recommendation: Utilize established risk management tools such as fault-tree analysis*

** Beutelschies, "That One's Gotta Work"* IEEE, 2001.*

Critical Fault Risk Management

Exercise #4: We can’t do that, so what will we miss?

What's the Risk?



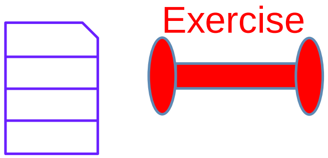
- **Tests not done**
  - *Week in the life end-to-end test*
- **Key characteristics not included in test**
  - *Weather*
  - *Altitude*
  - *Only 10% of counties participating*
- **Likely flaw path to mission failure**
  - *Poor shift handovers in new MCC*
  - *Throughput issues in new MCC on "bad day in the life"*

Fault Informed Risk Management

Candidate Test	Mission Objective	Test Objective	~ Test Duration	Key Characteristics	LYF Test Exceptions

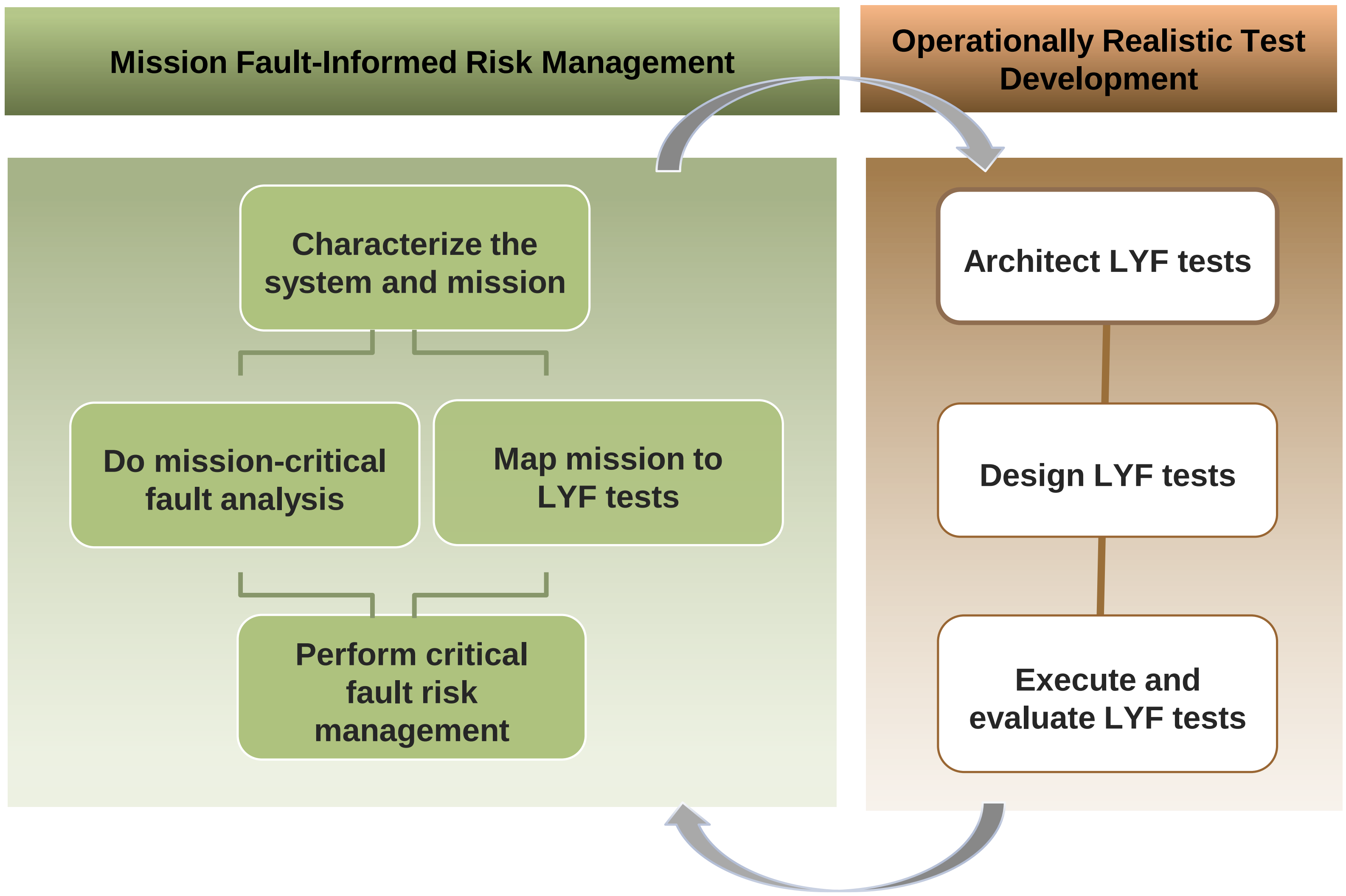
Identify at least one candidate test and as many attributes as possible in the table. You may use one candidate test identified before. Objective of exercise is to identify a likely test exception, up to and including not running the test.

If you are taking this session with colleagues, feel free to collaborate offline.



TLYF Process

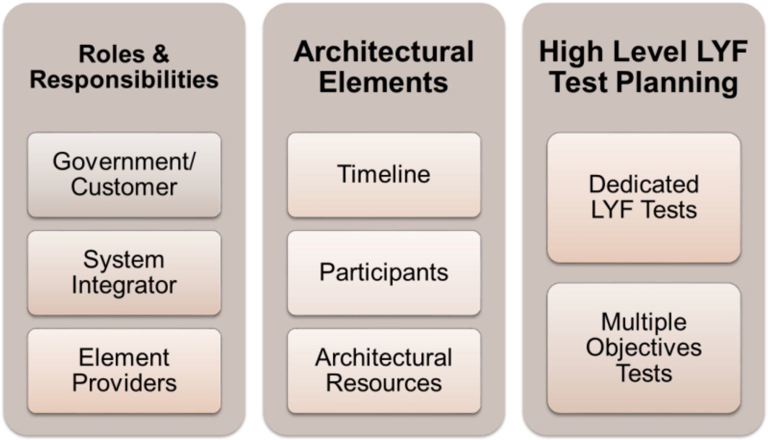
Test Development

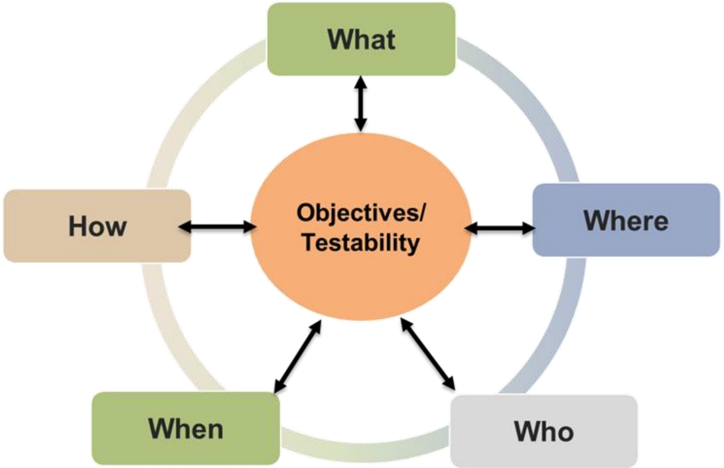


Architect LYF Tests

Description

- **Given the list of allocated LYF tests, develop the specific plans within the constraints identified**
- **Roles and responsibilities for involved organizations are established**
- **Key architectural elements for each test are formulated**
- **Create a high level test plan for each allocated LYF test involving all interacting elements**





Architectural Elements

Design, Execute and Evaluate LYF Tests

Design

Test Design Fidelity
- Operational HW & SW Use
- Fidelity to Mission Characteristics/ Configurations
- LYF Test Exceptions (Deviations from Mission)

Level of Test Specification (Pyramids)
- Mission Level
- HW & SW Integration

LYF Tests
- Test Objectives
- Incorporating Characteristics
- Test Processes & Procedures
- Success Criteria

Execute & Evaluate

Execute LYF Tests
- Test Level specification
- Documentation
- Participants
- Resources

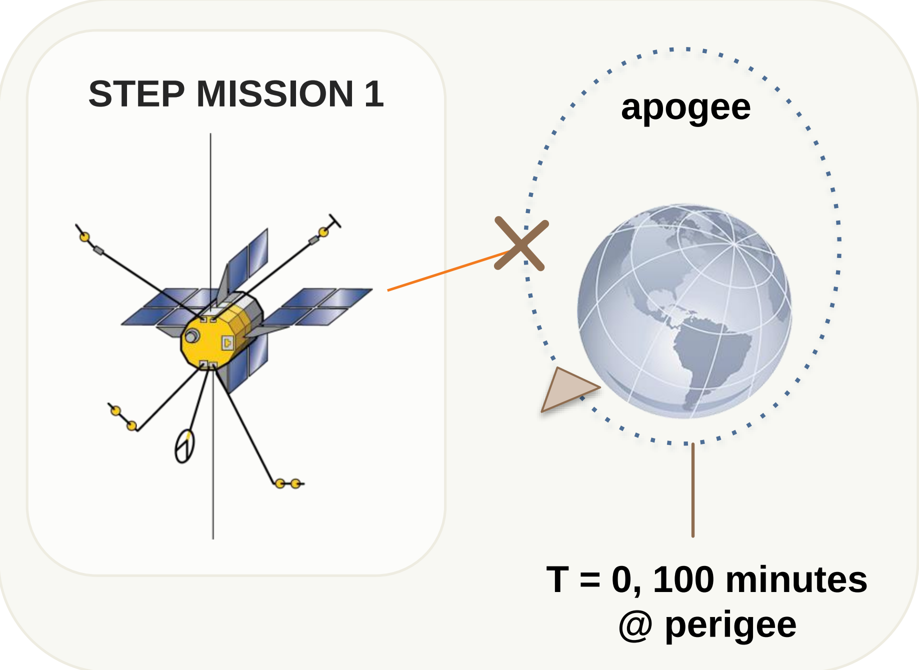
Evaluate LYF Test Results
- Data
- Reports
- Deviations from plan (redlines)
- Review

Lesson from STEP* Mission 1

Test Design as Function of Test Objectives

- STEP M1, with **one primary payload** & five secondary payloads, was to fly an 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
- **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*
- Very late in the test flow a LYF test 12-hour "Day-in-the-Life" test was added

*Space Test Experiment Platform

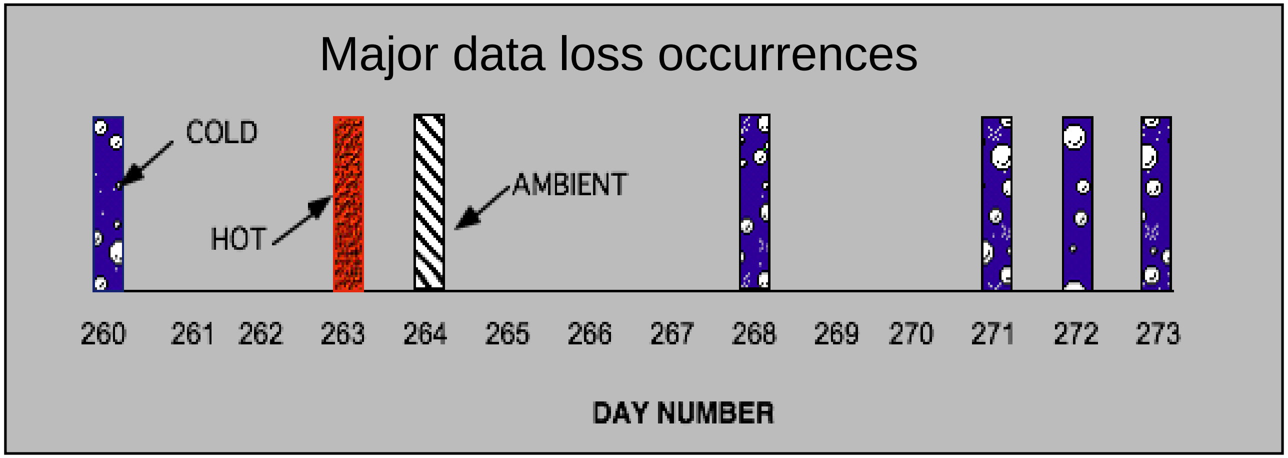


Diving Catch:
Loss of Primary Mission Data

LYF test objectives must be reflected in the test design.

ARGOS Thermal-Vacuum Operationally Realistic Test Results

- Space Vehicle days-in-the-life (DITL) test run as an overlay test during space vehicle thermal-vacuum test (240 hours of testing)
- Found that there were many mission data handling software errors and software / hardware interaction errors
- Would have led to excessive loss of data: failure to meet mission requirements



White, J. D., et al., Functional Test Success Criteria as Illustrated by the Space Test Program's ARGOS Satellite, 19th Aerospace Testing Seminar, United States Air Force/The Aerospace Corporation, Manhattan Beach, CA, 2000.

Design & Execute LYF Tests

Resulting Products

<u>Design</u>

- **Operationally realistic LYF tests**
- **For each LYF test, the following is generated:**
  - *Test plans (detailed with configurations and resources)*
  - *Test procedures*
  - *Entrance and exit criteria*
  - *Specific LYF test exceptions (i.e., detailed test deviations from mission, including impact from test equipment and resources)*

<u>Execute</u>

- **For each LYF test executed, the following is generated:**
  - *As-run (redlined) test procedures*
  - *Test results (report/data)*
  - *Discrepancy reports (DRs)*
  - *Additional LYF test exceptions (if applicable)*
  - *Additional flaws/faults discovered (if applicable)*
  - *Retest plans and procedures (if applicable*

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 not 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*

Courtesy of NASA/JPL-Caltech

Loss of Mission

Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions, JPL Special Review Board, March 22, 2000.

Identifying LYF Test Exceptions

- **Most of the work for LYF test exceptions are done in the design phase**

- **Initial exceptions often come from what is known to be available for testing**
  - *Flight article or simulator?*
  - *Operational interfaces or simulated?*
  - *Vehicle telemetry from test port, displayed on test equipment?*
  - *Software models?*

- **The criticality of LYF test exceptions can be determined if a MCFA has been performed**
  - *Any LYF test exception that is tied to a fault path will need to be addressed*

Q

Operational Resources and Test Resources

Differences Need to Be Accounted for

Mission/Operational

Tools

- *Command generation*
- *Operational Scripts*
- *Databases*
- *SOH Telemetry analysis*
- *Mission data conversion*

Process

- *Mission planning*
- *Command planning*
- *Data handling*
- *Contingency handling*
- *Discrepancy reporting*
- *Operational procedures*

People

- *Operators*

VS.

Test

Tools

- *Test Software*
- *Test Scripts*
- *Databases*
- *SOH Telemetry analysis*

Process

- *Command planning*
- *Test Data handling*
- *Contingency handling*
- *Discrepancy reporting*
- *Test procedures*

People

- *Testers*
- *System Designers*

The words may be the same, but the items are different

Like You Fly Test Exceptions

Premise

- **Doing tests exactly Like You Fly is usually not possible - there are likely to be several exceptions for every test of mission phase, mission timeline segment, and lower levels of the LYF pyramids**

- **Legitimate LYF test exceptions can arise from:**
  - *Physics—the test simply cannot be done*
  - *Engineering—it is not possible to perform the test without adding so much non-flight ancillary HW that too much uncertainty is added to the results*
  - *Programmatic reasons—due to cost, schedule, or other resource constraints*

- **LYF test exceptions are meaningful only when tied to specific operationally realistic LYF tests derived from the mission (mission mapped to operationally realistic LYF tests)**

Like You Fly Test Exceptions

Definition and Purpose

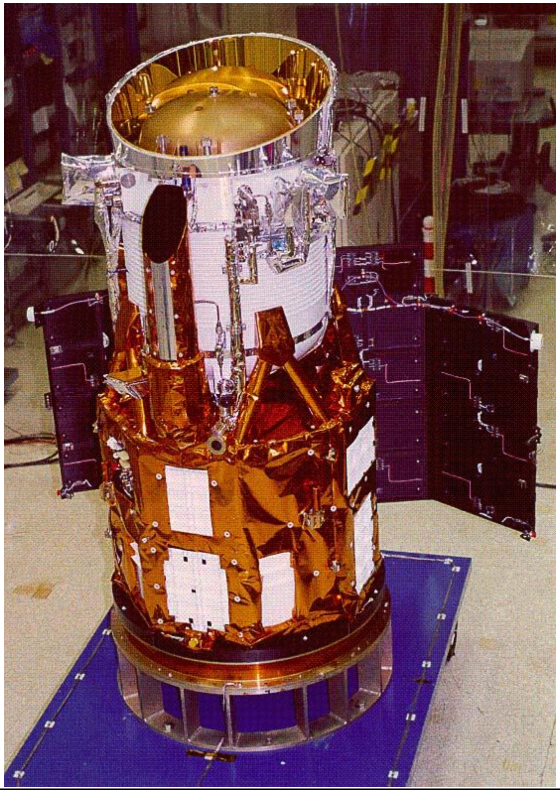
- **Definition**
  - *LYF Test Exceptions are **test deviations** from mission characteristics that apply to the mission activity under test*
  - *LYF Test Exceptions arise from 1) What we don't fly and 2) What we don't test*

- **Purpose**
  - *The deviations between the test-provided item/process and the mission critical characteristic(s) can mask flaws*
  - *Risk to mission arises when identified LYF test exceptions are linked with potential faults (Fault-informed path)*

Lesson from Wide-Field Infrared Explore (WIRE)

Test Substitutes Can Mask Fatal Design Flaws

- **Start-up transient in pyrocontroller caused premature telescope cover deployment allowing coolant to escape**
- **Lesson: Applicable mission / interface characteristics must be emulated or evaluated for differences between mission and test items**
  - *Timing*
  - *Start-up conditions*


Courtesy of NASA

WIRE

"… simulators and other support equipment used for design and verification tests lacked the fidelity required to detect this potential failure." WIRE Mishap Investigation Board Report, 1999

Loss of mission!

Architecting an Operationally Realistic Test

Exercise #5: Who, what, where, when and HOW?

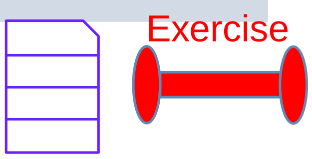
Instructions for Exercise: Architecting a LYF Test

- Pick a test identified in previous exercise to explore its architectural aspects
- Try to fill out as many items on the following table as possible
- If you are taking this session with colleagues, feel free to collaborate offline

Exercise

Architecting Operationally Realistic Tests

Allocated Test	Who should participate	What resources should be used	Where should each what reside	When must each item be available	How can this test event happen
Allocated Test	**Who has what role and responsibility**	**What portion of the mission timeline should be included**		**How long should the test be**	



Sample: High-Level LYF Test Exceptions

Allocated Test	Critical Event	LYF Test Objective	Mission Characteristics	LYF Test Exception

Identify any new LYF test exceptions that occur to you as a result of architecting the test.

If you are taking this session with colleagues, feel free to collaborate offline.

Exercise

Summary

- **The TLYF Process fosters smarter test design by using the mission as the basis and asking what could prevent mission execution success**

- **Following the process described promotes these sets of products for reducing mission risk:**

  – *Operationally realistic tests that are feasible, practical, perceptive, and value-added by addressing mission-critical events and system interactions*

  – *A list of critical events and associated fault paths and contributors (LYF test exceptions) that have either been exonerated or not*

  – *A fault informed set of remaining risks*

Summary

- **Mission based operationally realistic tests provide a clear roadmap to uncover flaws in the system prior to flight / fielding / use unlike other testing approaches**
  - *The mission-informed path and the fault-informed path help to efficiently and effectively identify the specific test parameters and conditions*
  - *These tests are identified, assessed, and allocated to the test program*
  - *LYF tests are architected, designed, executed, and evaluated*
  - *All identified mission-critical failure paths are either exonerated or revealed and mitigated*

- **The fault analysis offers decision makers a methodical approach for assessing the associated risks and determine how the risk will be managed**

Enhancing the chance of success at first usage!

Where to Go for More Information

- **Beutelschies, Guy. *That One's Gotta Work. Mars Odyssey's Use of a Fault Tree Driven Risk Assessment Process.* IEEE. Jet Propulsion Laboratory, Pasadena California, 2001**

- **"TOR-2014-02537-REV A - The Test Like You Fly Process Guide for Space, Launch, and Ground Systems" can be requested from the presenter**

Any Questions?

Thank you for your interest and attention