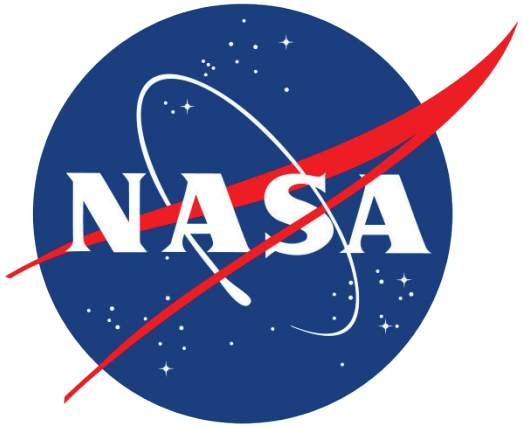
IV&V Dynamic Test and Analysis of the Orion Multi-Purpose Crew Vehicle FSW

2012 Annual Workshop on Validation and Verification

September 11-13, 2012



Presenters:

Ricky Beamer
frederick.m.beamer@ivv.nasa.gov

Eric Weasenforth
eric.d.weasenforth@ivv.nasa.gov

Additional Author:
Walter Schostak wschosta@purdue.edu

Agenda

- Background Information and History
  - ITC and the JSTAR Laboratory
  - MPCV Background and Overview
  - IV&V Analysis Challenges
- IV&V Dynamic Testing
  - Dynamic Test Capabilities
  - Test Environments and Tools Utilized
  - Example Demonstration Test Cases
- Summary and Path Forward

Background Information and History

ITC and the JSTAR Laboratory

- Independent Test Capability (ITC)
  - ITC team formed in the fall of 2009
  - Develop, maintain, and operate an adaptable test environment for the IV&V program that enables the dynamic analysis of software behaviors for multiple NASA missions
    - ITC = expert in simulation
    - IV&V Project = expert in specific systems
  - Provides an additional analysis tool that allows IV&V to ensure that the right behaviors have been defined and implemented to meet the users need under operational scenarios
    - Does the system do what it is supposed to do?
    - Does the system not do what the system is not supposed to do?
    - How does the system react under adverse conditions?
- Jon McBride Software Testing and Research (JSTAR) Laboratory
  - Created in January 2011
  - Provides advanced testing and evaluation capabilities

MPCV Background and Overview

- Based on the Constellation program's Orion design
- Capable of conducting regular in-space operations in conjunction with payloads delivered by the Space Launch System (SLS) for missions beyond LEO
- Potential backup system for International Space Station

Image Credit: NASA.gov

Orion Multi-Purpose Crew Vehicle

IV&V

Orion Summary

Number of crew 4
Crewed mission duration ..... 21-210 days
Total change in velocity ..... 4920 ft/s
Gross liftoff weight ..... 69,181 lbs
Effective mass to orbit ..... 50,231 lbs

Launch Abort System – Emergency Crew Escape System During Launch

Mass Properties

Dry mass/propellant ..... 10,369 lbs
Gross liftoff weight ..... 16,125 lbs

Crew Module – Crew and Cargo Transport

Pressurized volume (total) ..... 690.6 ft^3
Habitable volume (net) ..... 316 ft^3
Reaction control system (RCS) engine thrust ..... 160 lbf/engine
Return payload ..... 220 lbs

Mass Properties

Dry mass/propellant ..... 21,350 lbs
Oxygen/nitrogen/water ..... 77 lbs
Landing weight ..... 19,463 lbs
Gross liftoff weight ..... 21,650 lbs

Service Module – Propulsion, Electrical Power, Fluids Storage

Mass Properties

Oxygen/nitrogen/water ..... 694 lbs
Propellant weight ..... 17,433 lbs
Gross liftoff weight ..... 27,198 lbs

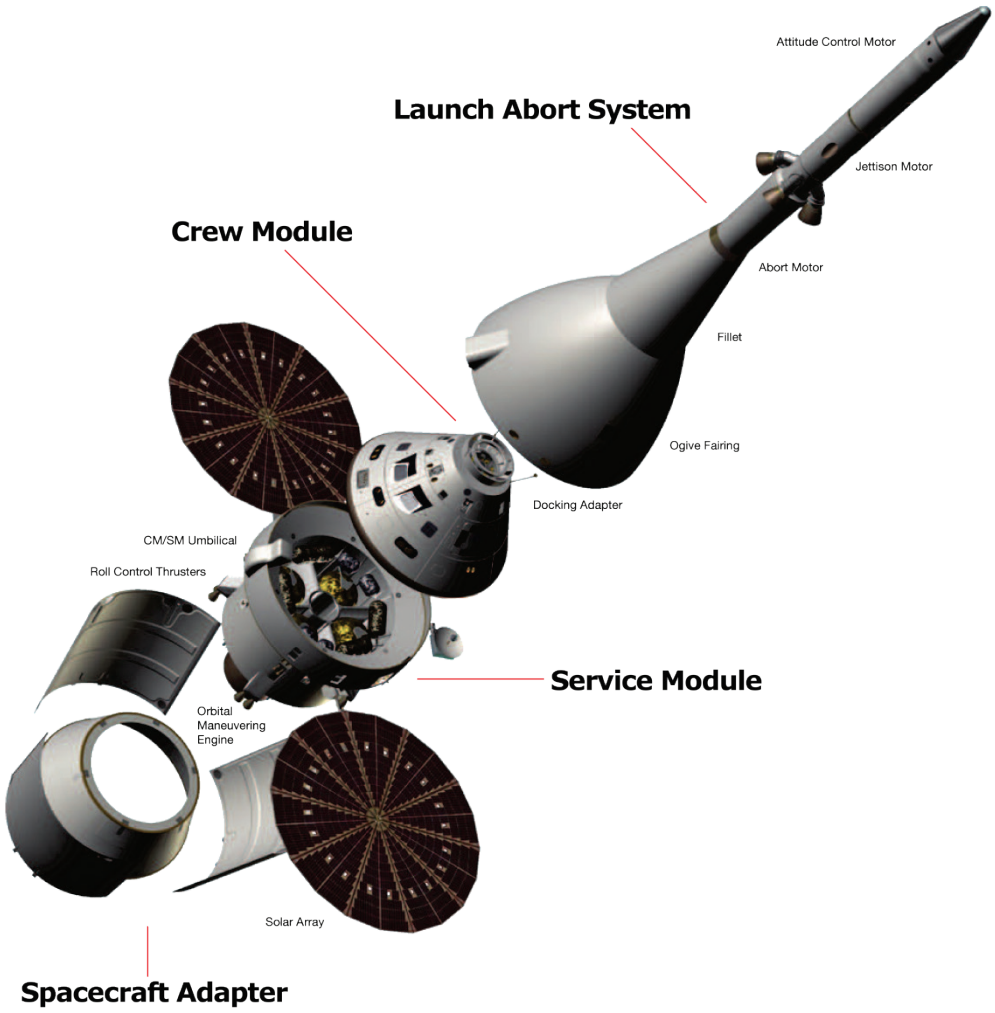


Image Credit: NASA.gov

IV&V Analysis Challenges

- Providing value while mitigating issues
- Inheritance of legacy code paradigm
  - i.e. non-conformity of source code languages
- Dual fault testing
- Run time regressing testing
- Complexity of FSW architecture increases the difficulty in analysis of behavior interactions

IV&V Dynamic Testing

Mitigating the Challenges & Achieving the Goals

Dynamic Test Capabilities
Mitigating the Challenges

- Dynamic testing provides IV&V the ability to perform functional level analysis
  - Captures system behaviors, design implementation, and interface definitions at a top level
  - Additional level of robustness over IV&V historical requirements, design, and static code analysis alone
  - Allows for refined classification and in-house mitigation and/or resolution of potential issues by providing substantiated evidence
  - Allows for supporting efforts by providing confidence and integrity checks against project systems
  - Scripting capability allows analysis of
    - multiple fault scenarios
    - complex interface designs

Test Environments and Tools Utilized

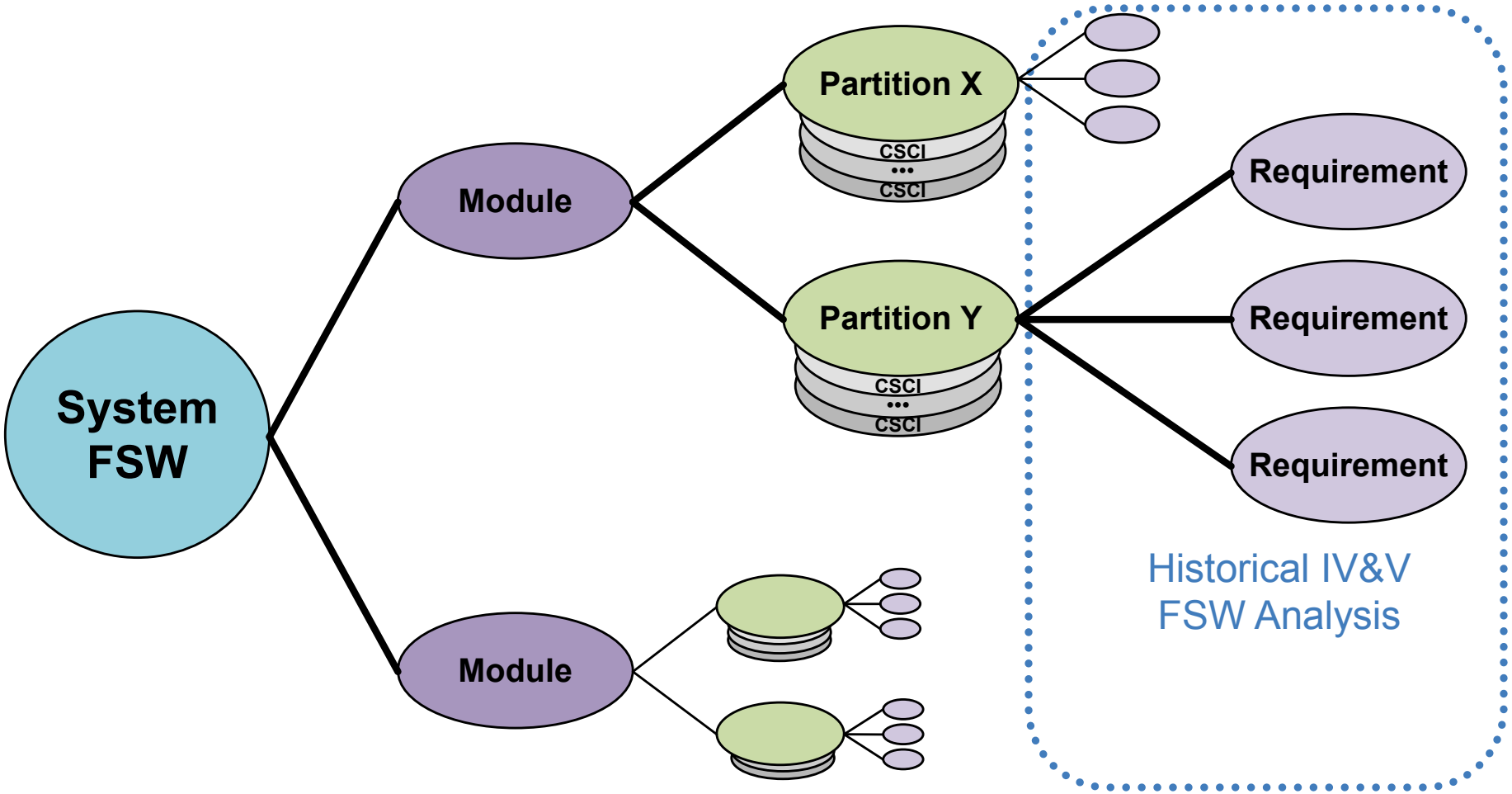
Available test environments for dynamic analysis

- **SOCRRATES** (Heavy and Lite) - *Software Only Crew Exploration Vehicle Risk Reduction Analysis Test Environment Simulation*
  - Developed by Lockheed Martin
  - Local instillation managed by ITC
  - No formal verification being conducted on the test environment
    - **SOCRRATES Lite** – *Simulation environment with the MPCV FSW modified and compiled to run on Linux*
    - **SOCRRATES Heavy** – *Simulation environment that executes the unmodified MPCV FSW on an emulated Simics target*

- **PLATO** - *Partition Level Application Test for Orion*
  - Developed by NASA at the Johnson Space Center
  - Local installation managed by ITC
  - Allows for execution of unmodified MPCV FSW on an emulated Simics target
  - Allows for single stepping through FSW in real time.

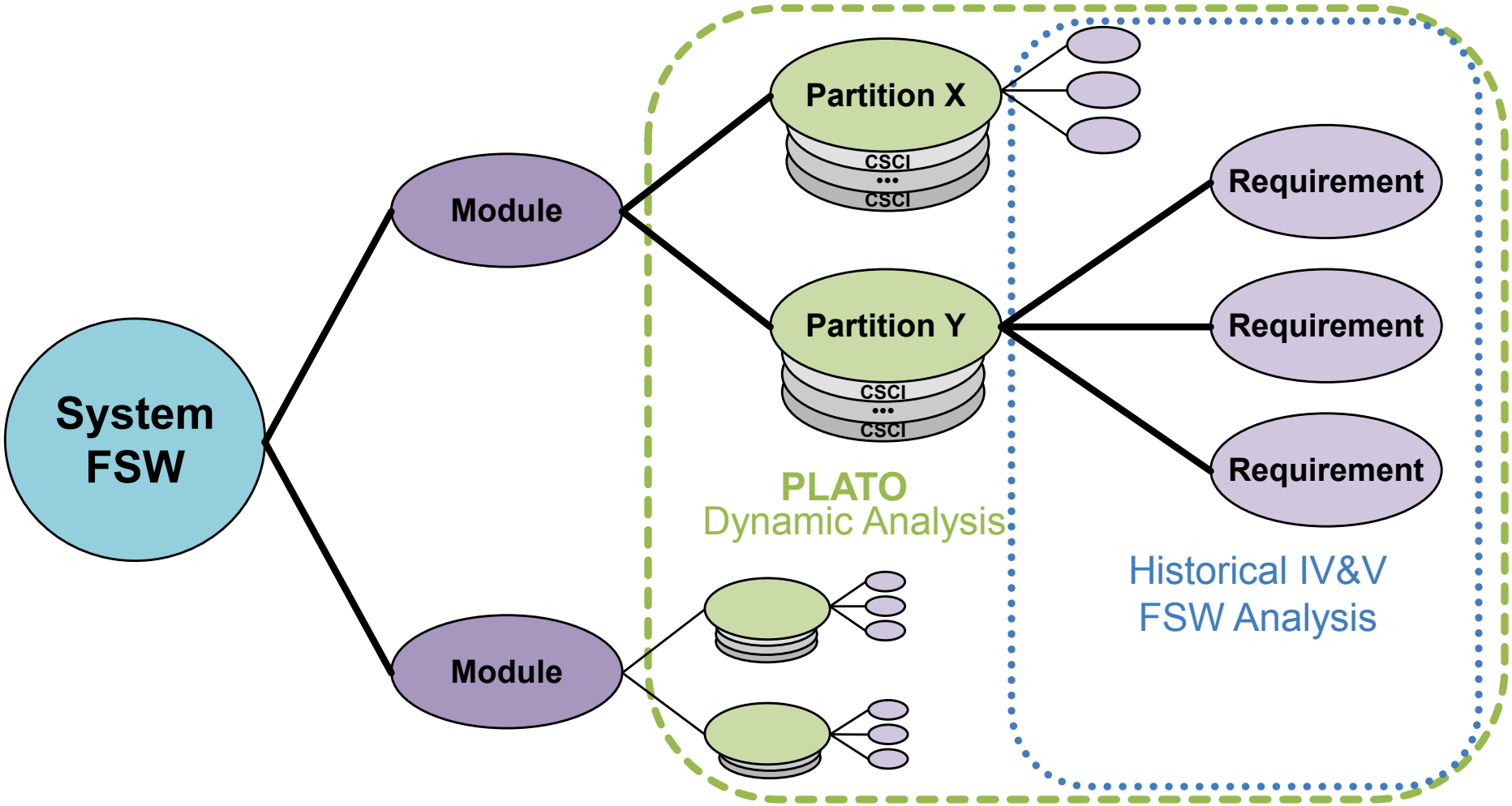
Test Environments and Tools Utilized

- Top level functional view



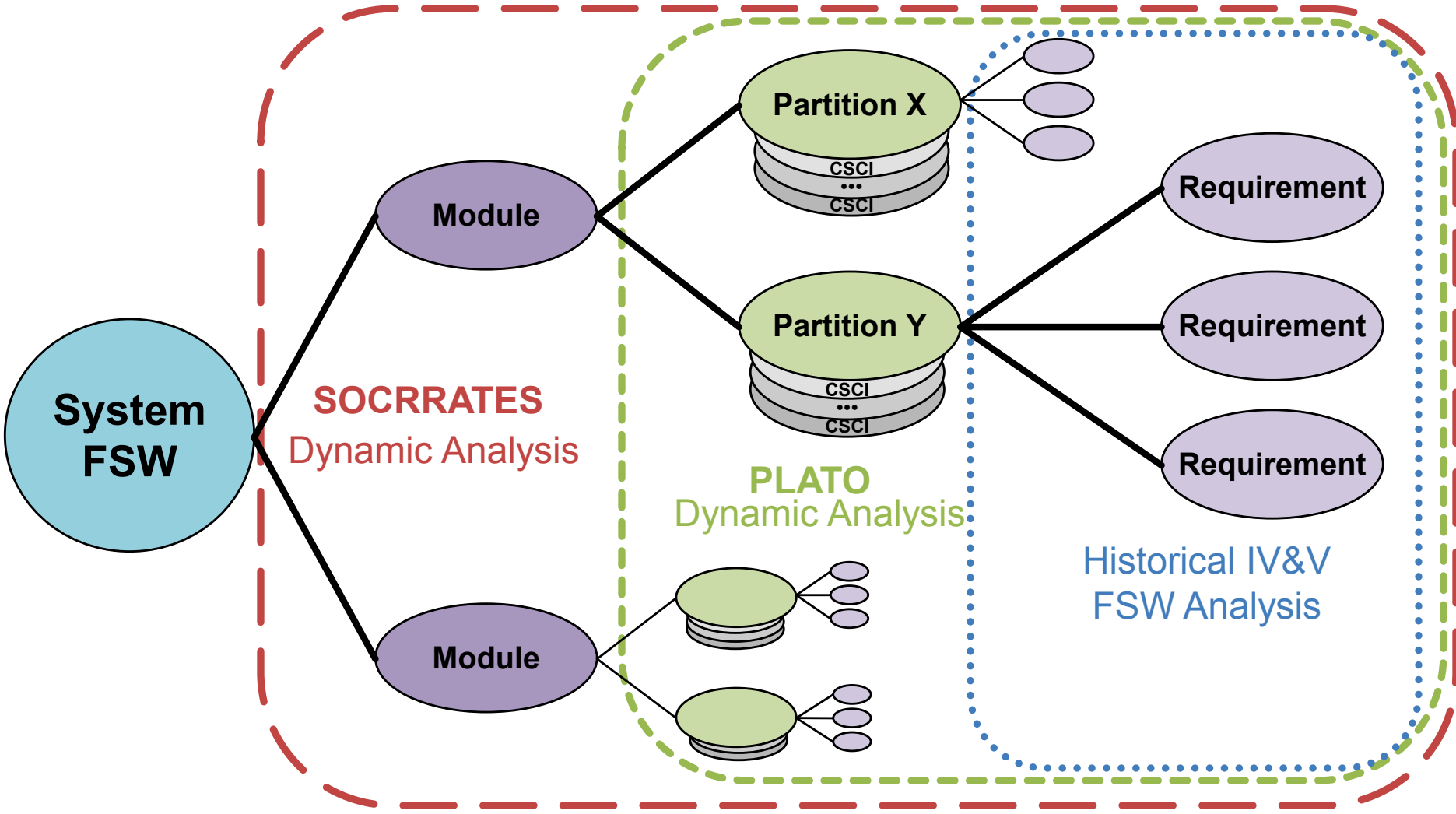
Test Environments and Tools Utilized

- Top level functional view



Test Environments and Tools Utilized

- Generalized top level functional representation



SOCRRATES Example Demo – Case 1

Functional Capabilities

Test Purpose

To demonstrate the system capabilities of SOCRRATES in a nominal setting. This is a test to determine similarity between a SOCRRATES-Lite and SOCRRATES Heavy run.

Initial Assumption

Nominal end-to-end test

Conditions

End to End Nominal Flight

Conclusions

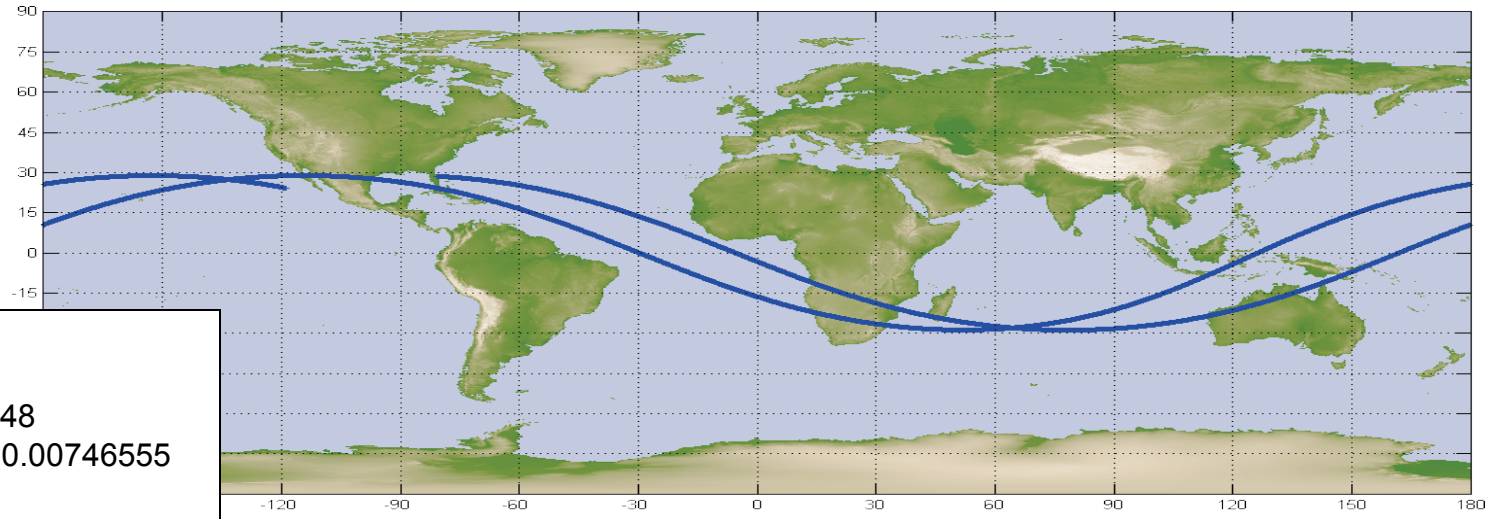
Based on the results, slight differences were discovered.

SOCRRATES Nominal End-to-End Results

IV&V

Baseline Graph of Lat/Lon

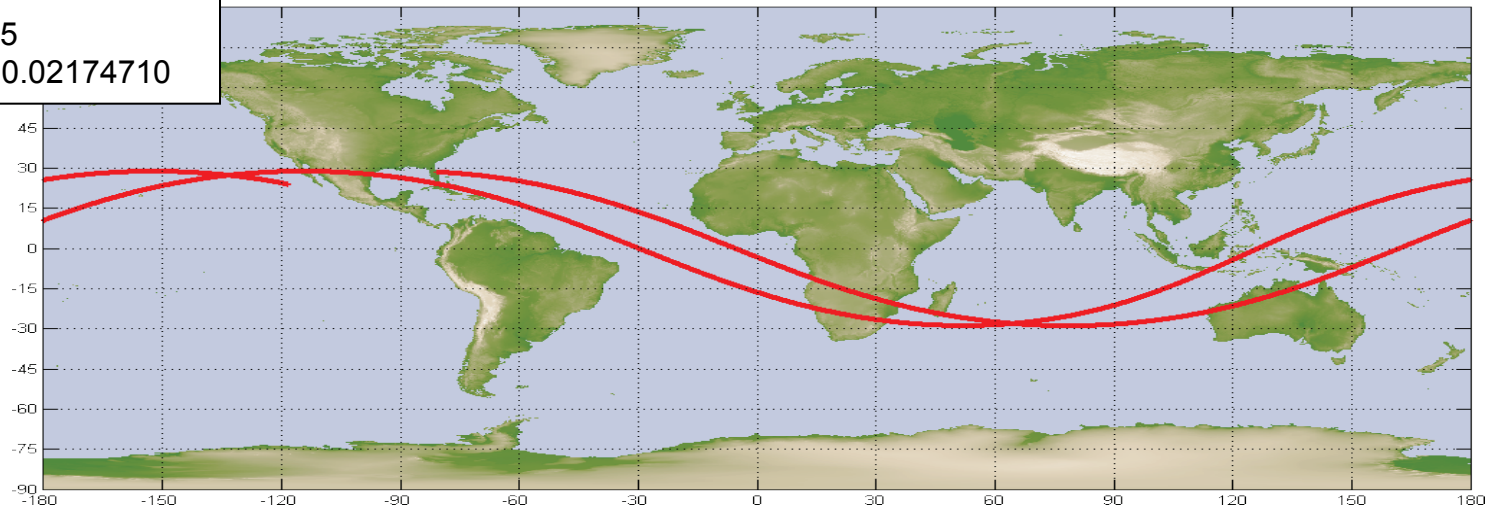
SOCRRATES-Lite



Divergence:
Latitude:
Average – 0.002100148
Standard Deviation – 0.00746555

Longitude:
Average – 0.01223505
Standard Deviation – 0.02174710

SOCRRATES-Heavy



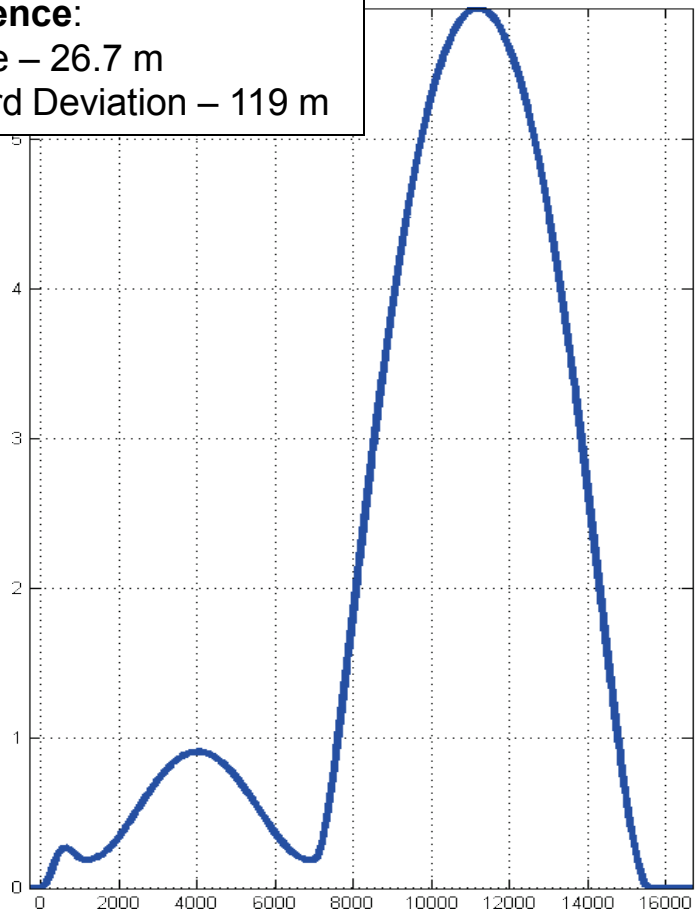
SOCRRATES Nominal End-to-End Results

IV&V

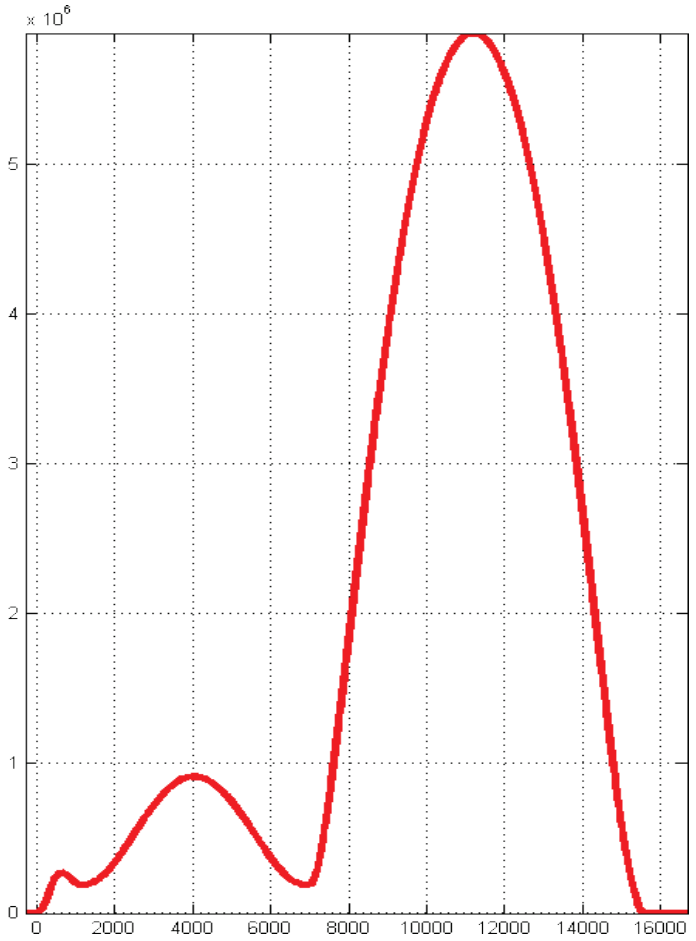
Altitude Profile Baseline Graph

SOCRRATES-Lite

Divergence:
Average – 26.7 m
Standard Deviation – 119 m



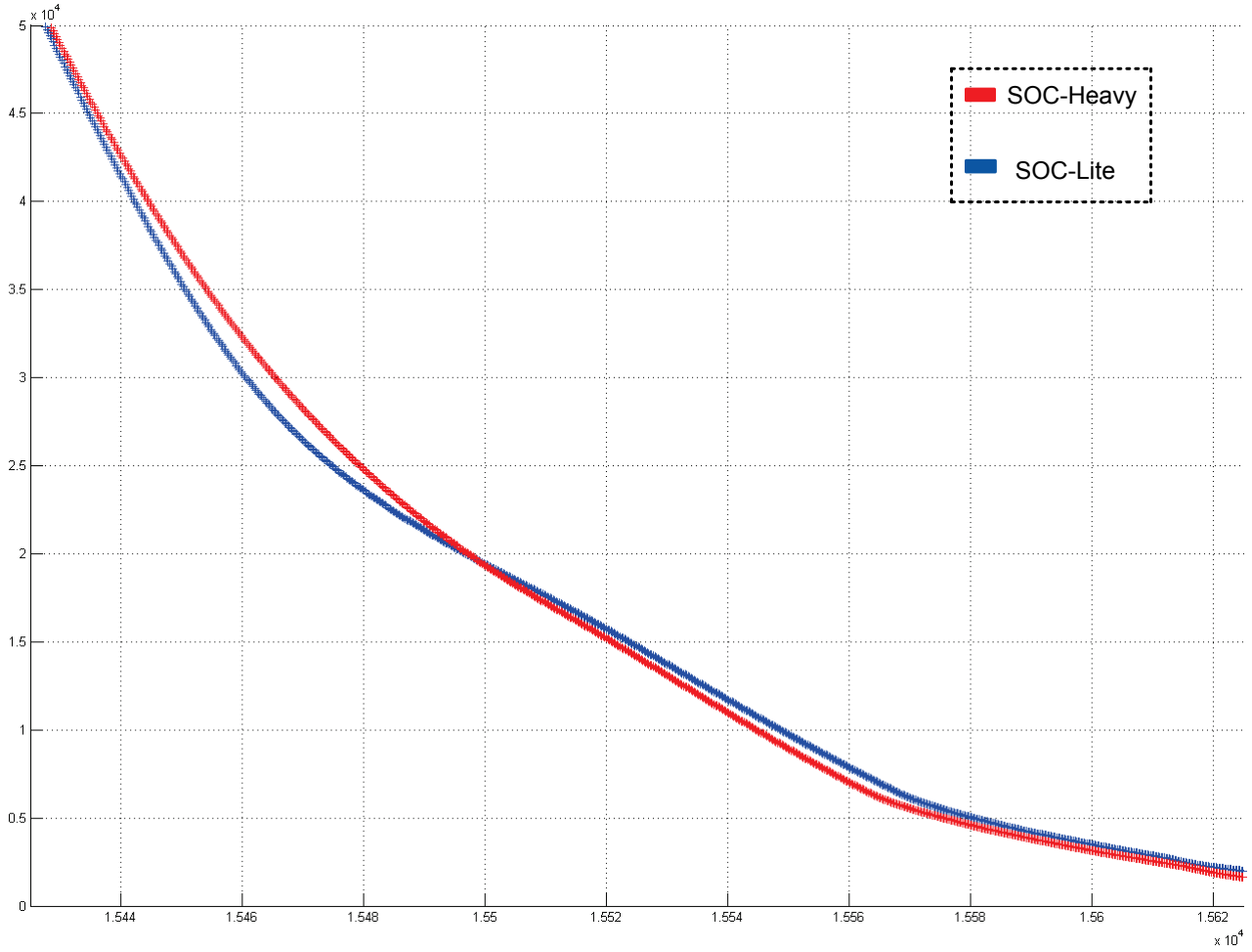
SOCRRATES-Heavy



SOCRRATES Nominal End-to-End Results

IV&V

- Additional slides from SOC Nominal run.



MPCV IV&V Test Goals

- IV&V dynamic testing to be conducted as an analysis tool and will run complimentary to MPCV formal and informal testing
- Not intended to duplicate testing being conducted by Lockheed Martin or by NASA
- Two main strategies for test approach
  - Scenario based (Nominal and Off-Nominal)
  - Multiple fault injection
- Other areas where tests can be generated
  - Historical IV&V analysis results
  - Issue severity determination
  - Stress Testing
  - Regression Testing

SOCRRATES Example Demo – Case 2

Analysis Tool – Fault Injection

Test Purpose

Within the global positioning system (GPS) flight software, a requirement exists that states once a set number of invalid data readings is reached, the system will no longer Identify the readings from that GPS as valid data. The purpose of this test is to show that the flight software reacts as expected to off-nominal conditions.

Initial Assumption

Since the craft has backup sensors, there will be no change in the telemetry data. However, there will be an observable change in the fault counts.

Conditions

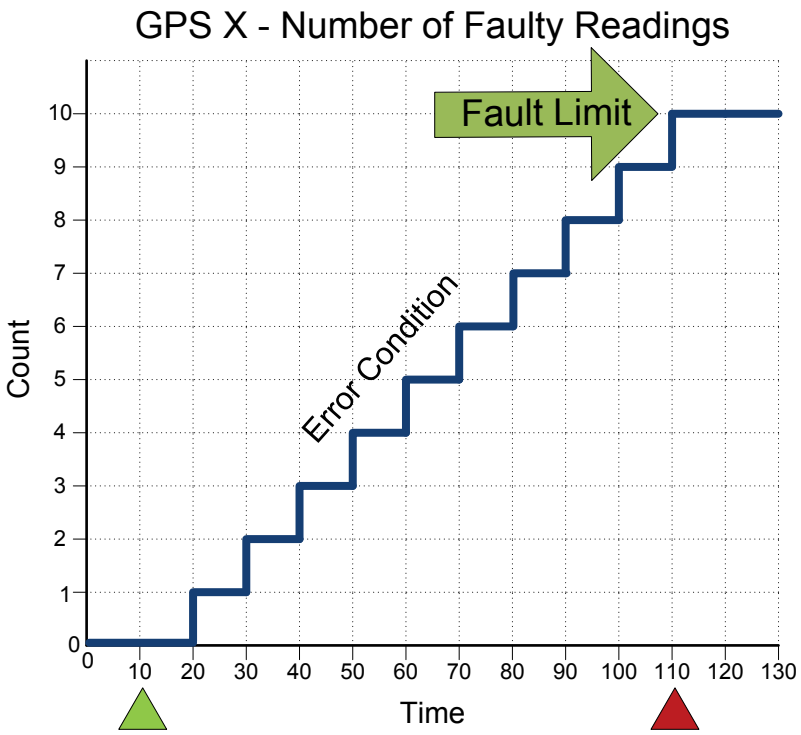
Nominal End to End flight with injection of a GPS fault script

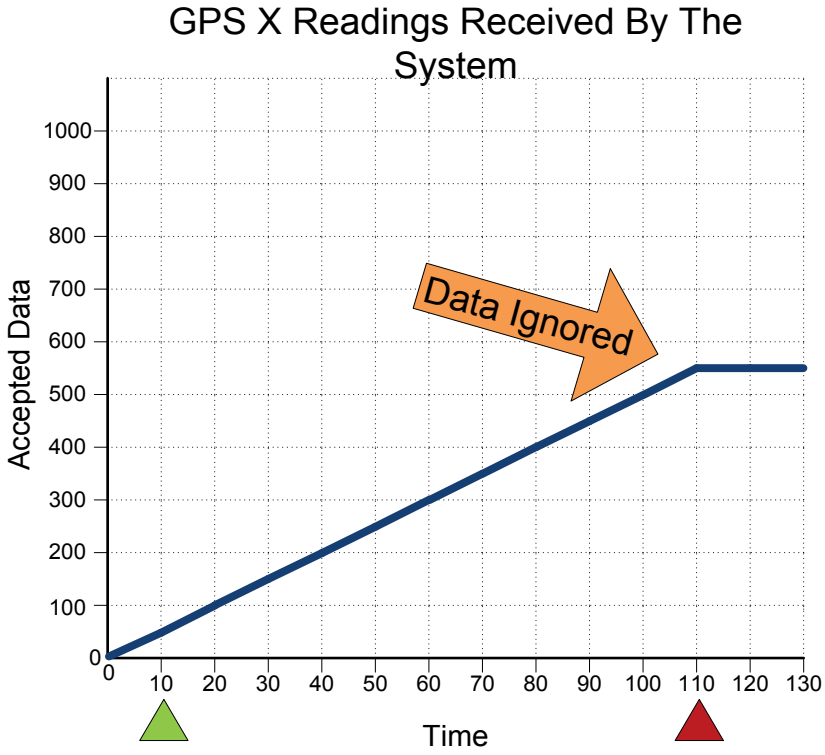
SOC-Heavy

Procedure

1. Incrementally increase the GPS fault counter via GPS fault script
2. Observe system response from script start through tolerance limit

SOCRRATES – Analysis Tool Example Results





- Script starts at 10
- Script runs for 100 seconds

Summary and Path Forward

Summary of Added Benefits

Static Analysis		Dynamic Analysis
Advantages	**Disadvantages**	**Advantages**
• Finds weaknesses in exact location • Allows quicker turnaround for fixes • Finds errors earlier in lifecycle ***Automated Tools*** • Relatively fast • Can scan all of code	• Can be time consuming • False Positives and False Negatives • Requires trained personnel • Do not provide runtime vulnerabilities ***Automated Tools*** • Can provide false sense of security • Only as good as rules they are using	• Finds run-time vulnerabilities • Provide increased flexibility of what to look for • Identifies vulnerabilities that may have been false negatives in static analyses • Validation of Static Analysis Findings • Dual Fault Testing ***Automated Tools*** • Inherent graphing capability • Helps to prevent false positives

Summary of Benefits for IV&V

- Test independently from the developer
- Provides ability to observe and evaluate behavior of the FSW under operational and environmental conditions
- Provide evidence based test results to support IV&V issues and severity assessment presented to the project
- Identification of improvement areas to the development test design
- Can investigate areas where IV&V feels additional test coverage would be beneficial
- Will give the project and IV&V more assurance that the software is working the way intended and reacts to adverse conditions properly
- Capable of regression testing in a more rigorous manner

A Look Forward

- Test environment as a common usable interface across all IV&V projects
- Based on success of SOCRRATES and PLATO as analytical tools, raise awareness for future integration and use of simulation tools
- More robust and thorough test plan under development
- Will continue to refine testing goals
- Will gather and generate test cases as analysis continues
- Future analytical work with PLATO and SOCRRATES

BACKUP

EFT-1 - MPCV

IV&V

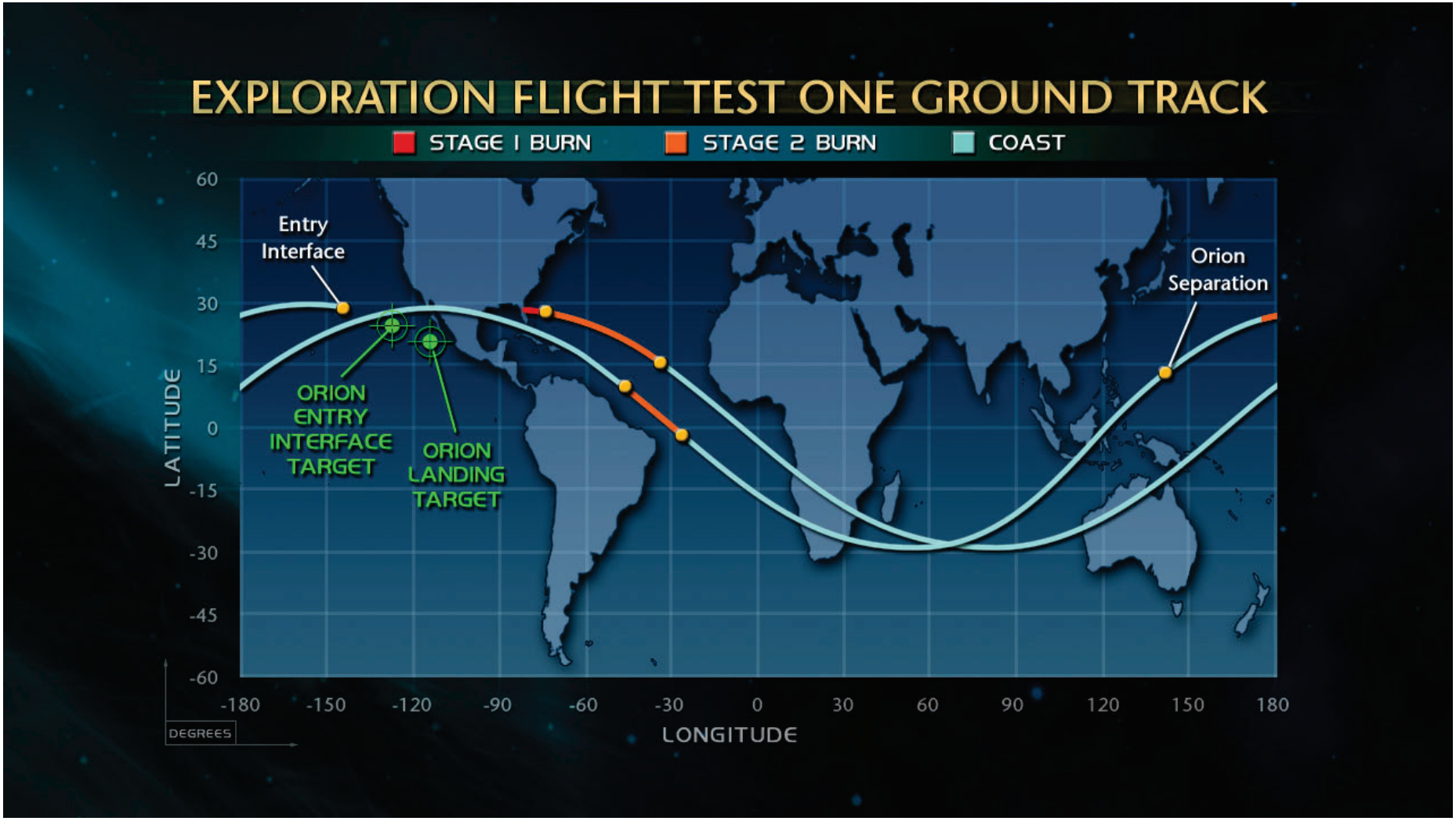


Image Credit: NASA.gov

EFT-1 - MPCV

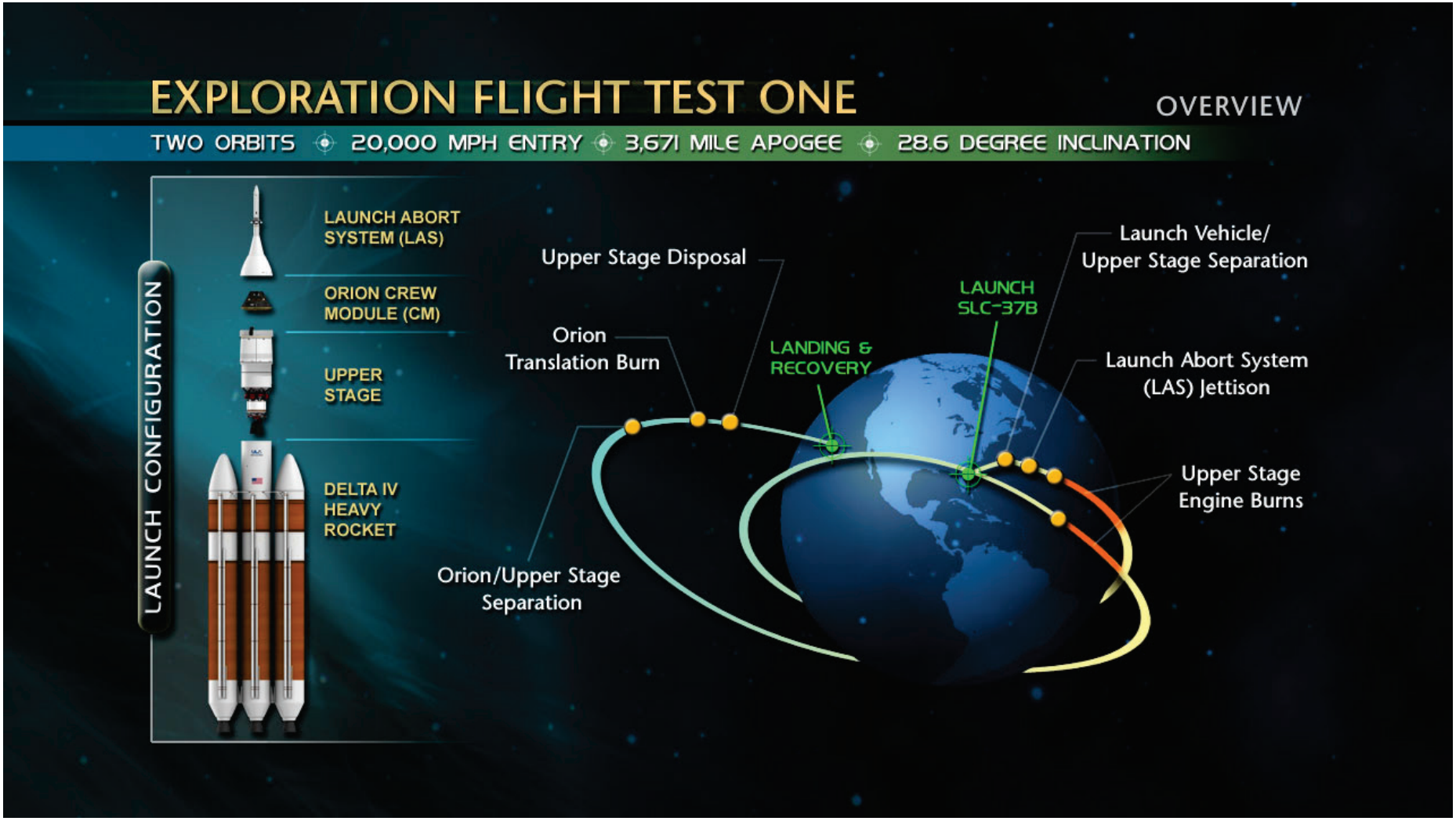


Image Credit: NASA.gov