Automated Generation and Assessment of Autonomous Systems Test Cases

Kevin J. Barltrop
Kenneth H. Friberg
Gregory A. Horvath

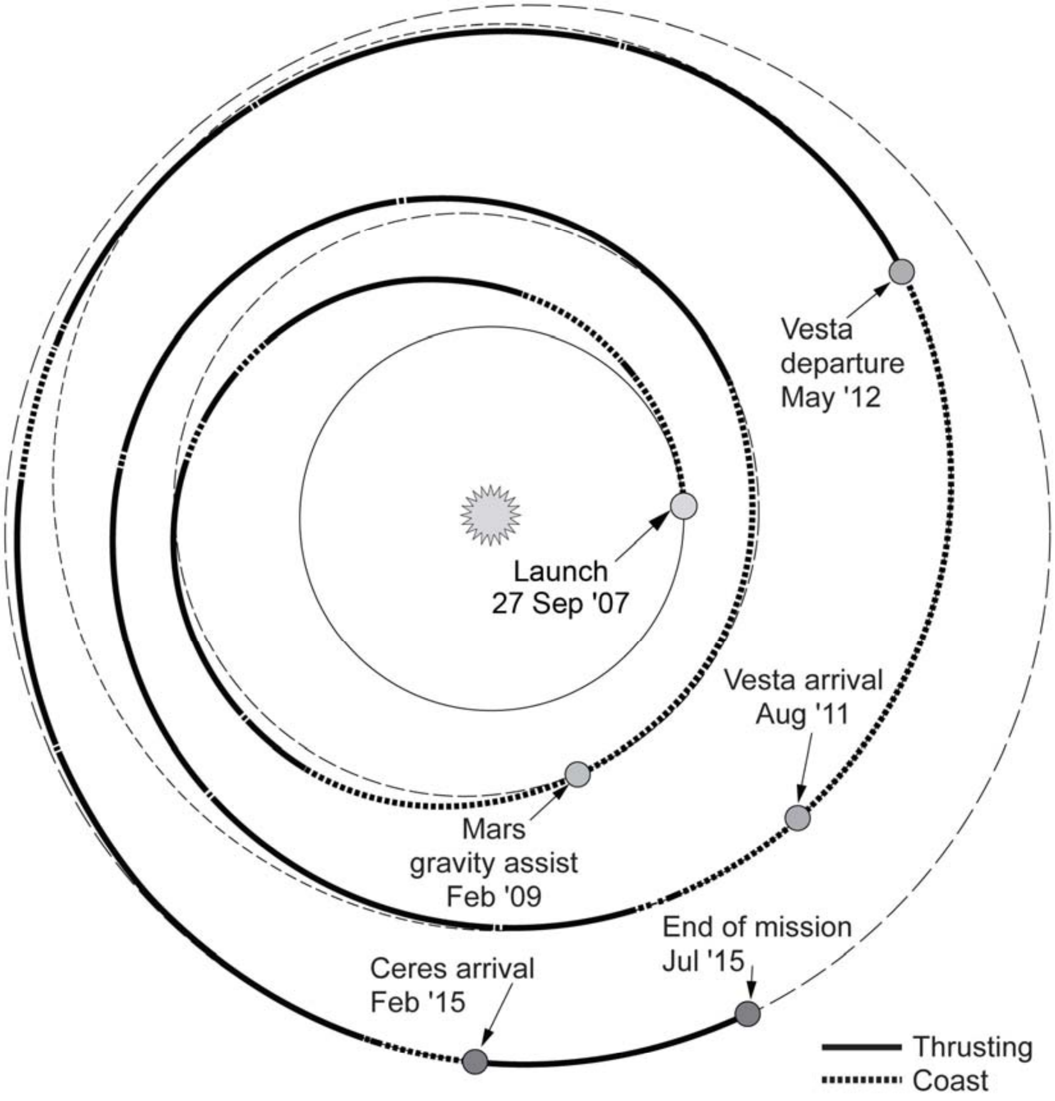
Jet Propulsion Laboratory
California Institute of Technology

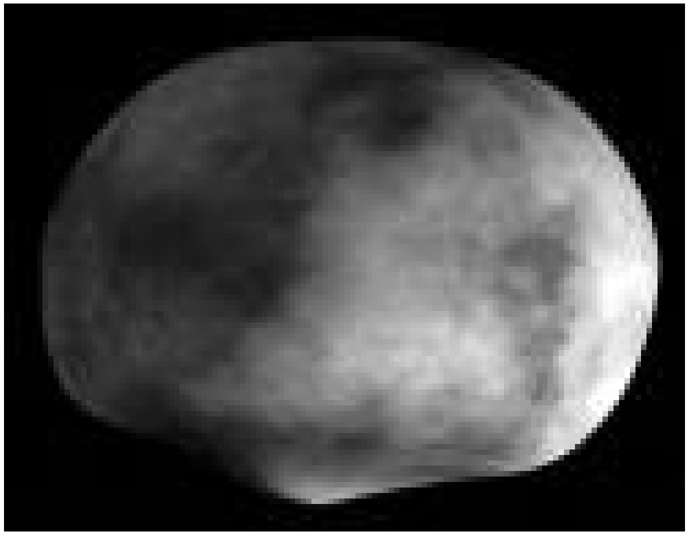
March 3 2008

Presentation Overview

- Dawn Mission Overview
- Problem Statement: Dawn Fault Protection (FP) Testing Challenges
  - “Gee, that’s a lot of tests”
- The Solution: Automated Rule-Based Test Case Analysis
- Results
- Conclusions and Recommendations
- Author Bios

Dawn Mission Overview





Dawn Mission Overview (cont’d)

- Dawn's goal is to characterize the conditions and processes of the solar system's earliest epoch by investigating in detail two of the largest protoplanets remaining intact since their formations. Ceres and Vesta reside in the extensive zone between Mars and Jupiter together with many other smaller bodies, called the asteroid belt. Each has followed a very different evolutionary path constrained by the diversity of processes that operated during the first few million years of solar system evolution.

Dawn FP Testing Challenges

- From a design and implementation standpoint, the Dawn FP design is ‘simple’
  - Launch vehicle separation and solar array deployment is the only time critical event – all other fault scenarios are of the ‘safe and wait’ variety
  - All parameters are table values
  - All responses are sequential command sequences stored as software tables
- The simplicity, however, can be deceiving – ‘the devil is in the details’
  - The Dawn FP design has no architecturally supported method for managing these complex behaviors and their resultant interactions
  - Rather, these behaviors are managed by targeted enabling and disabling of potentially conflicting monitors and responses
  - Further expanding the test space is the fact that the architecture allows for parallel response execution
  - Complicating matters further are complex interactions between FP and the Attitude Control (ACS), Power (EPS), and Thermal (TCS) subsystems
- ***We must rely heavily on test data to properly ‘tune’ the system and reduce the risk of false detections and***

Automated Test Case Generation

Automated Test Case Assessment

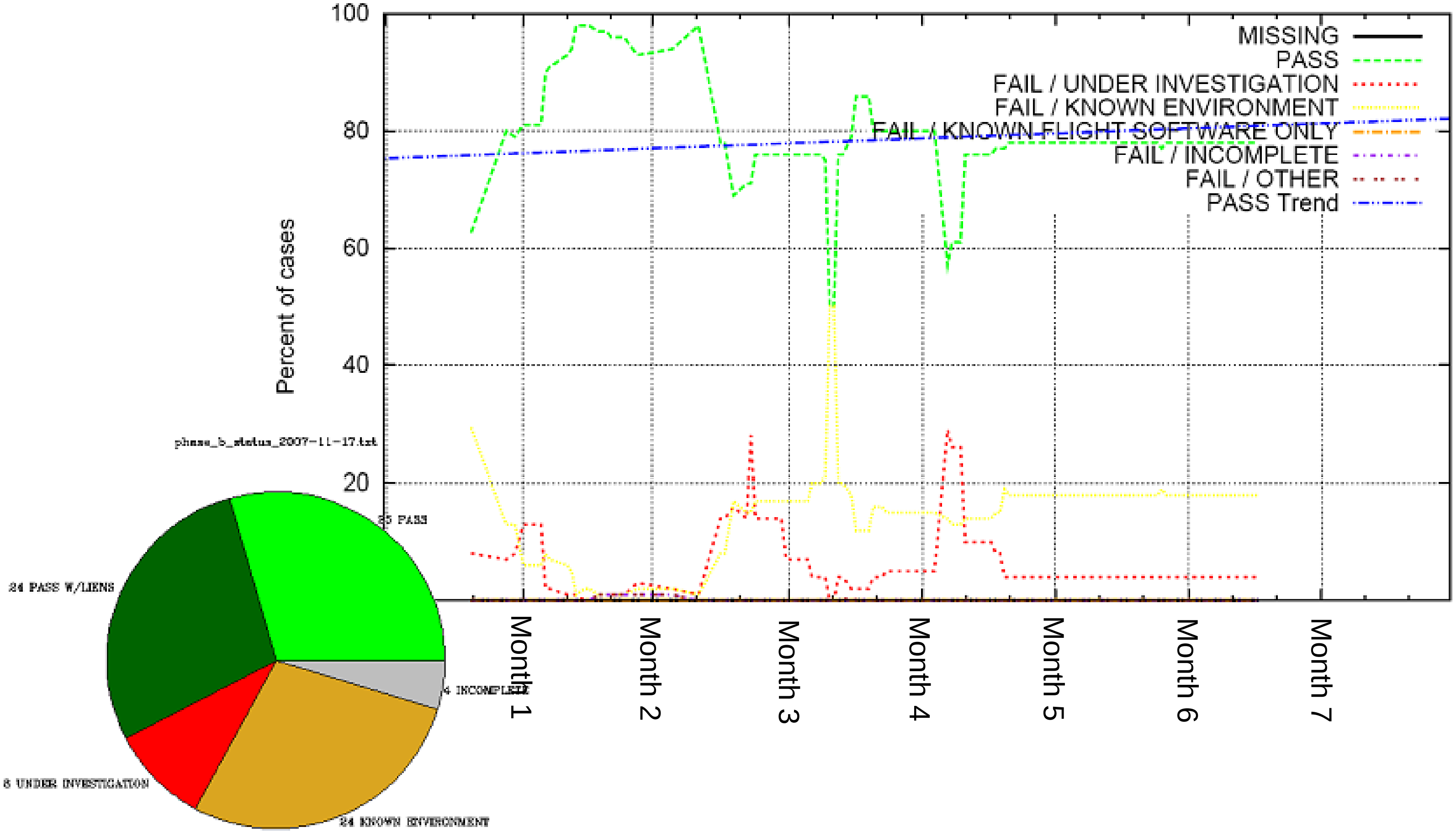
- The objective of the automated test case evaluation was to provide a means to identify recurring problems and prioritize cases for follow-up investigation.
- Key level 2 requirements were selected as the basis for the pass/fail subvector.
- The assessment is performed by computing a vector that scores the test results against a set of proscribed criteria concerning those requirements.
- For all fault injections identified by failure modes and fault tree analysis in combination with any unintended fault injections identified by failure modes and fault tree analysis, the spacecraft shall achieve an end configuration that satisfies all end state constraint rules.
  - *Criterion 1:* Achieve configuration that satisfies all constraint rules.
  - *Criterion 2*: Never command the spacecraft to a hazardous configuration.
  - *Criterion 3*: Achieve stable state for a period of at least 30 minutes.
  - *Criterion 4*: No unexplained fault detections and responses occur.
  - *Criterion 5*: No conflicting commands.

Automated Test Case Assessment (cont’d)

- Assessments were performed using several different analyses:
  - Count of events of interest
    - Flight computer reboots
    - Number of active response sequences
    - Alarms, etc…
  - Thread analysis
    - Identify individual chains of events within scenario.
    - Evaluate step-by-step states commanded by each chain of events.
    - Identify conflicting commanded states.
    - Identify flight rule violations

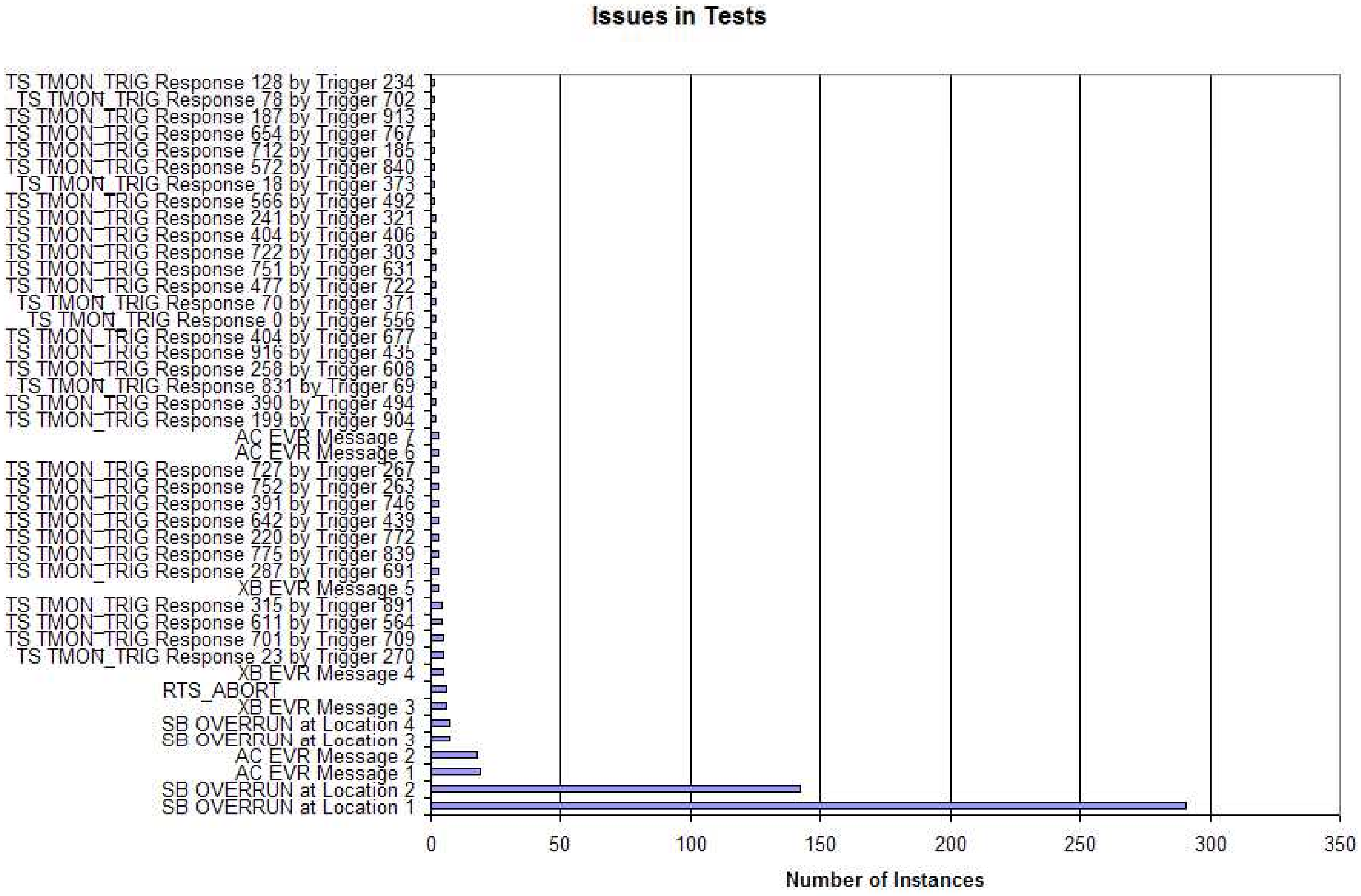
- Assessments presented in several ways:
  - Table of scoring vector for each scenario
  - Graphs with trends for different classes of problems
  - Histograms showing distributions of problems.

Representative Mid-Campaign Results



s0.s1.s2.s3.s4.s5.s6.s7.s8	=	0	1	4	18	16	0	0	0	0	0*	0	0	1	4	1	5

Representative Results (cont’d)



Conclusions and Recommendations

- The use of automated test generation, execution, and evaluation was instrumental in validating the Dawn fault protection design.
- The Dawn activities are a next step in a path towards more capable closed-loop end-to-end system testing.
- As a follow-on, JPL has begun to apply additional techniques to Dawn:
    - Adaptive testing in which an intelligent test harness uses evolutionary computing and modeling of the mission to evolve scenarios that flush out weaknesses in the system.
    - Model checking that evaluates correctness of the system behavior around selected scenarios.

Author Bio: Kevin Barltrop

- ***Kevin Barltrop*** *is a Senior member of the Systems Engineering Autonomy Group at JPL and served as the FP test analyst for the Dawn Mission. In addition to his Dawn work, he previously served as the FP Architect and Systems Lead for the Deep Impact Mission, the AACS FP Lead for Cassini, has supported a number of JPL institutional research activities into improved systems engineering methods for fault protection, and served on numerous review boards. Before coming to JPL in 1998 he spent seven years in GPS and GPS-automation research at Stanford Telecom on contracts for the FAA, NASDA, and ESA projects. He has an M.S. in Aerospace Engineering (Dynamics and Control) from the University of Michigan, and a B.S.E. in Aerospace Engineering from Virginia Tech.*

Author Bio: Ken Friberg

- ***Ken Friberg*** *was a Senior member of the Systems Engineering Autonomy Group at JPL and had been at JPL for 14 years and built Communication satellites at Hughes Space and Communications Co. (now Boeing Satellite Systems) for 5 years. Past projects include autonomy leads on Dawn, Cassini, and TDRS (H,I,J) and work on Galileo attitude control, the BSS702 commercial satellite bus and the Europa/X2000 project. He has focused extensively on deep space dual-string autonomy with an emphasis on attitude control and ground automation. He also has worked on state model-based software architecture. He has a BSE in engineering physics and aerospace from the University of Michigan and is currently starting up a ground-based autonomous robotic company in Portland, OR – Friberg.Autonomy@gmail.com*

Author Bio: Greg Horvath

- ***Greg Horvath*** *is a Member of Engineering Staff at NASA's Jet Propulsion Laboratory (JPL) in Pasadena, CA. He holds a BS in Computer Science from New York University and a BE in Electrical Engineering from Stevens Institute of Technology. Since joining JPL full-time, Greg has had a variety of positions, giving him a broad knowledge of the issues affecting deep space missions and the technologies associated with them. As a member of the MDS team, Greg participated in are-engineering of the MDS software frameworks, and assisted with a prototype integration of the Titan reasoning engine into the MDS framework. As a member of the Deep Impact Fault Protection team, Greg helped guide the twin Deep Impact spacecraft to a successful encounter with Comet Tempel/1 on July 4, 2005. Presently, Greg is the Fault Protection Operations Lead for the Dawn mission to asteroids Vesta and Ceres.*