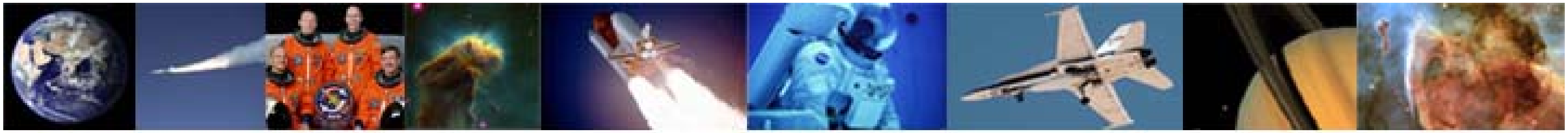


Fender Bender: DART’s Automated Collision

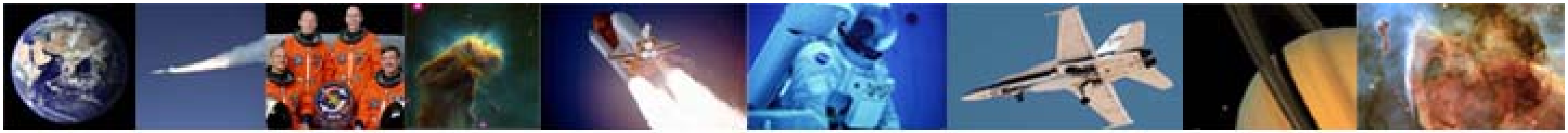
Leadership ViTS Meeting
September 2008

Bryan O’Connor
Chief, Safety and Mission Assurance

Jim Lloyd
Deputy Chief, Safety and Mission Assurance

This and previous presentations are archived at:

http://pbma.nasa.gov/pbma_main_cid_584



Space Collision

- The Demonstration of Autonomous Rendezvous Technology (DART) spacecraft launched on April 15, 2005, with pre-programmed instructions to rendezvous with the Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM) satellite and perform close-range maneuvers without the assistance of ground control at any point during the mission.

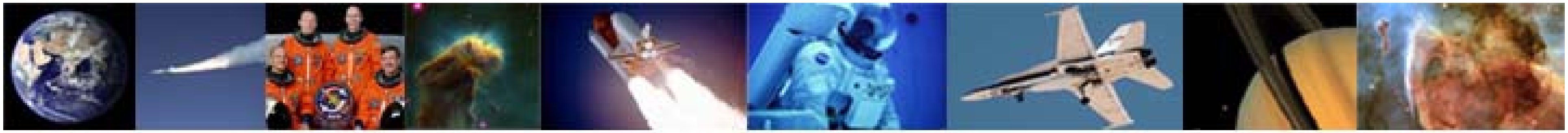
- DART used its Advanced Video Guidance Sensor (AVGS) in conjunction with three GPS receivers to calculate its velocity and position relative to MUBLCOM so that DART could fire its thrusters accurately during rendezvous. For the close-range maneuvers (proximity operations), the navigational control for DART was to switchover completely to AVGS.

- Due to errors in its software, the navigational system could not accurately determine DART's velocity or position. While rendezvous was successful, excessive (and inaccurate) thruster firings depleted DART's fuel supply faster than expected.

DART (foreground), MUBLCOM (background)

- During proximity operations, the software errors caused DART to miss the critical waypoint needed to switchover its navigational control completely to the AVGS.

- Approximately 11 hours into the 24 hour mission, DART collided with MUBLCOM. Shortly afterwards, its fuel supply ran out, and DART transitioned to its Departure and Retirement sequence without having accomplished any of its 14 technology objectives.



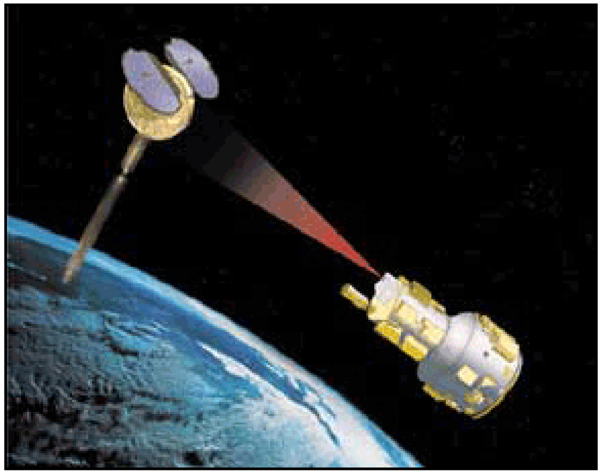
Software Specification and Validation

- To determine DART’s velocity and position, its navigational system compared software-based estimates (based on GPS) with measurements (GPS and AVGS) using a relative weighting system, or “gain.” If the estimates differed from the measurements beyond a set tolerance, the software would “reset” and estimate again.

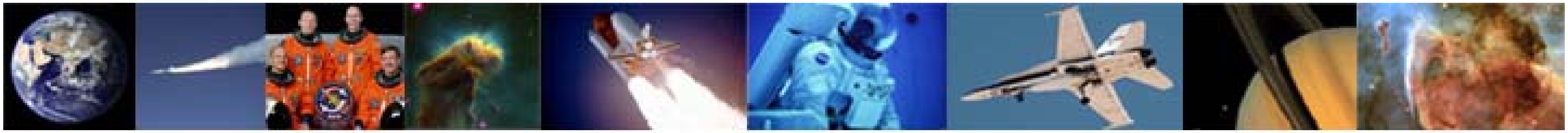
  Error 1: The comparison of the velocity input from the GPS receiver to the software-based estimates had to be within an accuracy of ± 1 m/s or the estimates would diverge from the measurements and trigger a reset. However, the GPS design specified the accuracy to ± 2 m/s. The allowed imprecision sent DART into an infinite do-loop, resetting itself about once every 3 minutes.

  Error 2: The gain setting was changed close to launch to accommodate for a unit conversion error found late in the testing phase. The new setting gave an inappropriately high weighting to the estimates relative to the measurements. While the original gain setting would have broken the infinite-loop bug from Error 1, the new setting perpetuated it … and nobody caught it.

- The improperly designed and executed navigational system software prompted excessive and inaccurate thruster firings, causing DART to miss the waypoint needed to trigger switchover to AVGS navigational control. If switchover had occurred as planned, the GPS data would have been ignored, and the reset loop would have been broken.



DART (right) used estimates and measurements to determine its velocity and position relative to MUBLCOM (left).

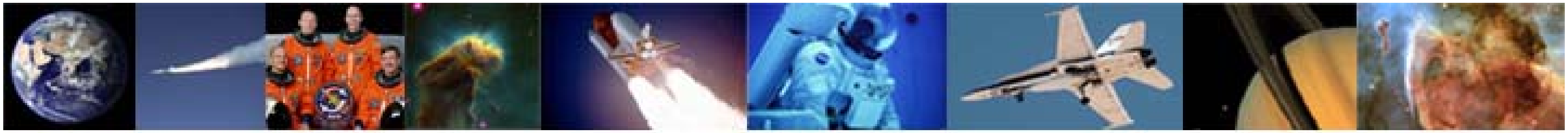


Proximate Cause

- The inability to accurately determine its velocity and position resulted in excessive and incorrect thruster firings that caused DART to collide with its rendezvous partner.

Root Cause/Underlying Issues

- Poor requirements not challenged by software validation nor detected through software verification
  - Requirements for the accuracy of GPS velocity were outside of the tolerance window that the navigational software could realistically accept. The potential infinite-loop scenario had been identified, but a software fix was not implemented because it was not fully understood that the GPS data would be used in this way.
  - The use of GPS velocity as the input to the software estimates was not adequately documented or communicated to the operations staff, so tests of the software code never included using the GPS inputs to update the estimates.
  - Modified gain settings applied an inappropriately high weighting to the software estimates. These settings had not been properly tested or verified due to proximity to the launch date.
- Ineffective design choices
  - The command sequences utilized a heritage software architecture that was later determined inadequate for autonomous space operations because of its lack of adaptability to unanticipated inputs.
  - DART did not have the capability for any ground control. While philosophically consistent with an autonomous demonstration, it left no margin for error and no provision for rescue.
- Lack of training, experience, and oversight
  - The Mishap Investigation Board cited a lack of training and experience for the inadequate design and testing, as well as the ineffective use of subject matter experts and lessons learned to challenge the design.
  - DART was classified as a high-risk, low-budget mission and therefore most of the design decisions were left to the contractor with little government oversight. Even as costs ballooned to $110 million and the mission importance increased, no additional levels of validation or review were added to ensure mission success.



Lessons Learned for NASA

- Flight critical software benefits from early validation of requirements. Does the software:
  - Do what we want it to do?
  - Not do what we do not want it to do?
  - Perform properly in contingencies?

- Independent audits, assessments, and peer reviews are valuable tools to ensure that proper testing, procedures, and safeguards are in place and have been properly documented and communicated. It is critical to review the training, experience, and capabilities of the project teams, including contractors.

- Program and project management should regularly review the risk level classification of a mission to accommodate for potential shifts in the risk tolerance with changing conditions. As programs mature and become higher visibility, a “high-risk, low-budget” posture may no longer be appropriate.

- Program and project teams should employ subject matter experts and apply previously learned lessons in order to fully leverage NASA’s wealth of past experiences. Specific tools or references and lessons learned found to be valuable should be acknowledged, so that other program and project teams can benefit from them as well.