National Aeronautics and Space Administration

System Failure Case Studies

SEPTEMBER 2008 Volume 2 Issue 7

FENDER BENDER

The Demonstration of Autonomous Rendezvous Technology (DART) program began in May 2001, intending to demonstrate that a spacecraft could independently rendezvous with an orbiting satellite without human intervention. In April 2005, the DART spacecraft was successfully launched with both Phase I (Launch and Early Orbit) and Phase II (Rendezvous) considered successful. However, following a series of navigational system errors and problems with fuel management, DART crashed into its rendezvous partner spacecraft. Shortly afterwards, the mission prematurely ended without having achieved any of its Phase III (Proximity Operations) technical and scientific objectives. DART transitioned into Phase IV (Departure and Retirement) only 11 hours into its 24-hour mission plan. Analysis showed that multiple design errors and testing issues in the navigational system contributed to what NASA declared a "Type A" mishap.

BACKGROUND

The DART program began in 2001, designated as a high-risk technology demonstration project, and was assigned to the Orbital Space Plan (OSP) Program in 2002. The OSP Program was cancelled following President George W. Bush's announcement of the Vision for Space Exploration, but DART continued due to the maturity of the program and the relevance of autonomous rendezvous technology to in-space assembly.

For an overall cost of more than double what Orbital Sciences Corporation (OSC) initially proposed ($110 million versus $47 million), DART was designed to conduct pre-programmed autonomous rendezvous and maneuvers with a target satellite already in orbit named Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM). The DART mission was intended to lay the foundation for future manned and unmanned missions that could use computers rather than humans to perform space operations. Prospective applications included cargo delivery, servicing missions to the International Space Station, and other space activities.

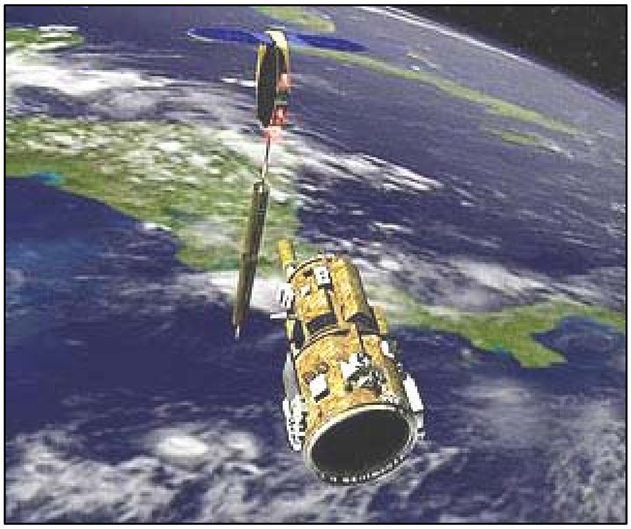

Figure 1: Artist rendition of the DART spacecraft (foreground) in orbit with the MUBLCOM satellite (background).

The DART Mission Plan consisted of four phases: (I) Launch and Early Orbit, (II) Rendezvous, (III) Proximity Operations, and (IV) Departure and Retirement. In the Rendezvous phase, thrusters on DART would perform a timed burn to bring the spacecraft to within 1 km of MUBLCOM and then approach the satellite to within 200-500 m during the ensuing Proximity Operations phase. Here, DART would perform a number of close-range maneuvers including pre-planned holds, docking axis approach, and circumnavigation. Finally, the vehicle

In April 2005, DART crashed into the satellite with which it was designed to rendezvous.

Proximate Cause:

- Inaccurate measurement of speed and distance resulted in the collision and premature loss of fuel

Underlying Issues:

- Lack of software validation and verification allowed an infinite-loop of navigational system resets
- Numerous design flaws included inappropriate gains settings, misuse of heritage software architecture, and low margins for error
- Lack of training, experience, and oversight of the project team and prime contractor

was to demonstrate a collision avoidance maneuver before the spacecraft departed from MUBLCOM and ejected its remaining fuel to enter a retirement orbit (the Departure and Retirement phase).

The navigational system consisted of pre-programmed, autonomous software logic designed to use inputs from both an Advanced Video Guidance Sensor (AVGS) on DART and three Global Positioning System (GPS) receivers (two on DART and one on MUBLCOM). Utilizing a complex algorithm to combine the data from the AVGS and GPS sensors, the navigational system would calculate the velocity and position of DART relative to MUBLCOM to determine when and for how long to fire its thrusters. After the Rendezvous phase and when in range to conduct the Proximity Operations phase, DART needed to pass through a critical target area in order to trigger the navigational system to stop using the GPS sensors. The intent was to test the performance of planned close-range maneuvers using only the AVGS, which alone could collect navigation data from signals reflected off of MUBLCOM and use this data to make calculations about DART's relative range, bearing, and attitude. Thus, throughout the mission, DART would operate autonomously and guide itself without any commands from ground personnel.

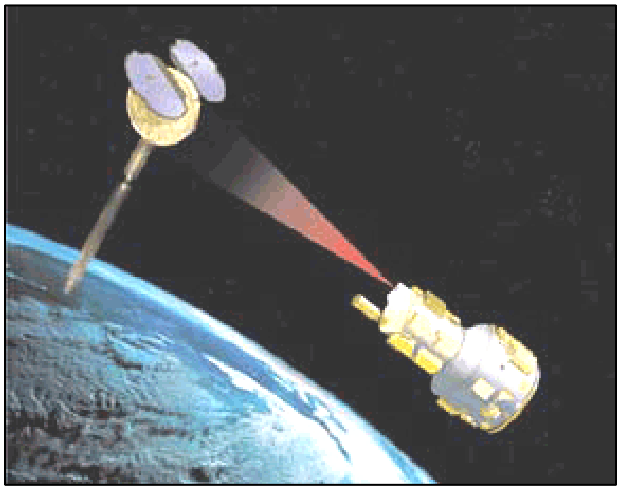

Figure 2: DART's (right) AVGS gathers data from laser signals reflected off MUBLCOM (left) in order to calculate range, bearing, and attitude (artist rendition).

WHAT HAPPENED?

On April 15, 2005, DART was carried with its Pegasus launch vehicle by aircraft to 40,000 feet over the Pacific Ocean where it was released. The Pegasus rocket, built by OSC, then ignited and carried DART more than 450 miles above Earth to an initial parking orbit near MUBLCOM, which concluded the first phase of its mission. During the subsequent rendezvous with MUBLCOM, a number of anomalies occurred within DART's navigational system, including excessive thruster firings and fuel usage, which were noted by ground personnel. Despite these anomalies, DART achieved its initial objectives for both Phases I and II within the first eight hours of the 24-hour mission. However, as Phase III operations commenced, major problems began.

The Collision

During the Proximity Operations phase, it became clear to ground personnel that DART's fuel was being spent at a rate that would cause a premature end to the mission. Errors in the navigation data from the GPS were causing excessive (and incorrect) thruster firings, and DART missed the critical target area that was needed to trigger the navigational system's switchover to use the AVGS without the GPS sensors. Due to the completely autonomous nature of DART, ground personnel had no means to remedy this situation. With the faulty navigation data, DART did not have an accurate measure of its velocity and distance relative to MUBLCOM. Approximately 11 hours into the mission, DART collided with MUBLCOM. Shortly thereafter, DART detected its low fuel supply and transitioned to Phase IV without completing any of its Phase III mission objectives. MUBLCOM was not significantly damaged and was returned to operational status, but DART failed to accomplish any of the 14 Phase III critical technology objectives, resulting in its classification as a “Type A” mishap.

PROXIMATE CAUSE

Due to errors in its software, the navigational system could not accurately measure DART's position and velocity relative to MUBLCOM. In fact, when DART hit MUBLCOM at 1.5 m/s, its navigational system was reporting that it was 130 m away traveling at 0.3 m/s in the opposite direction. The same software errors also resulted in excessive thruster firings, which depleted DART's fuel and brought a premature end to the mission.

UNDERLYING ISSUES

Software Requirements and Validation

The navigational system was programmed to constantly compare its own software-based estimates of spacecraft position and velocity with measurements from the navigational sensors (AVGS and GPS). If the difference in values was outside of a predetermined tolerance window, the software discarded the estimated position and velocity and then re-estimated these parameters using the GPS data as input (a “reset”). However, DART's GPS receivers consistently provided a velocity measurement outside of the tolerance window. This was due to an initial design requirement specifying that the velocity measurement only had to be accurate to within 2 m/s, when in reality the Mishap Investigation Board (MIB) found that a discrepancy of less than 1 m/s would trigger a reset.

The MIB reported that this infinite-loop scenario was actually a known “bug,” but the DART team never implemented a software fix because most of the staff was not even aware that DART’s GPS velocity output was being used in the software estimates. The MIB determined that the use of GPS data in this way was the product of a flight code change that had not been adequately documented and that the pre-flight simulation and testing protocol had never taken this change into account. As a result, the navigation software was actually resetting itself about every three minutes throughout the mission. The MIB Public Release established that the continual resets were responsible for the incorrect navigational data.

Ineffective Design Choices

In addition to accepting too wide of an accuracy range in the GPS output velocity (as described above), the MIB Public Release identified a number of other flawed design specifications due in part to a combination of schedule pressures and improper testing.

The navigation software calculated the difference between the estimates and measurements (and thus, the need for a reset) by using a relative weighting, called the “gain,” based on the comparative importance of the two data. Close to the planned launch date and late in the testing phase, the gain setting was changed to optimize performance during Proximity Operations. However, the MIB discovered that this new setting had given an inappropriately high weighting to the estimates relative to the measurements. They also concluded that the original gain would have broken the infinite-loop reset bug, whereas the changed setting actually perpetuated it. The MIB stated that this change was not properly tested or verified due to schedule pressures associated with the launch date.

For the pre-programmed, timed sequence of commands, OSC reused the software architecture from its Pegasus launch vehicle. The MIB ultimately found that this software was inadequate for autonomous space operations because of its lack of adaptability to unanticipated inputs. Additionally, the MIB declared that the 18 m wide target area chosen to activate the complete switchover to AVGS was too small. Due to the navigation errors, DART missed the undersized area by less than 2 m. Had the switchover to AVGS been completed as planned, the navigational system would have no longer been affected by the inaccurate GPS data.

Finally, the system design did not provide the ability for ground operators to issue any commands to DART once in space. While this was considered philosophically consistent with the mission objectives to display autonomous behavior, it also ensured that any mistakes would be unrecoverable.

Training, Experience, and Oversight

The DART MIB specifically noted that the lack of training and experience of the DART team (both government and contractors) resulted in inadequate design and testing, failure to utilize subject matter experts and lessons learned documented from past NASA projects, and insufficient technical communication due to misperceptions regarding International Traffic in Arms Regulations (ITAR) restrictions. Inadequate systems engineering was cited to be a “significant causal factor,” with a reference to performance requirements not containing enough detail to preclude numerous possible interpretations for systems that may not integrate properly. For example, the tolerance for the accuracy of the GPS velocity output was set higher than the navigation software could realistically accept. Also, the gains levels were supposedly optimized for Proximity Operations performance but actually magnified the effects of the navigational system errors.

Due to the high-risk, low-budget designation of the DART mission, NASA had set broad requirements and left most of the details and design decisions up to the discretion of the contractor. However, even as the DART mission progressively became a more high-profile milestone for NASA, it was still never reclassified. The MIB concluded that the prime contractor’s (OSC) internal system of checks and balances failed to identify key issues responsible for the mishap and that the lack of government oversight led to inadequate assessment of technical risk and insufficient use of independent testing and peer reviews.

AFTERMATH

Both spacecrafts remained in orbit after the mishap, so there were no direct inspections made of DART or MUBLCOM after the collision. NASA classified DART as a “Type A” mishap, which is designated by a mission failure exceeding $1 million in losses. Due to ITAR and Export Administration Regulations (EAR) restrictions, the MIB issued a Public Release instead of the complete official mishap investigation report. The Public Release summarized the results of the investigation and included a list of root causes as well as a series of recommendations.

The MIB recommended the NASA Research Acquisition (NRA) approach be modified to apply only to initial conceptual design phases of technically-complex, high-profile missions and called for greater government control and detail in specifications for key design decisions. NASA Headquarters disagreed with the finding, stating that the NRA needed only appropriate levels of management rigor and peer review. To this, the MIB suggested that peer review procedures require independent check of the utilization of lessons learned documentation and that

NASA centers with technical responsibility obtain independent audits or reviews of their capabilities.

LESSONS LEARNED FOR NASA

The DART mission met or partially met only 11 of its 27 total mission objectives. But the MIB noted that the experience gained from actual design and operation was crucial in identifying the deficiencies in the current autonomous spacecraft rendezvous techniques. The principle failure was a result of improper software settings. Flight critical software benefits from early validation of requirements, and the DART mishap highlights the importance of software specification and verification. The simulations used to test DART's flight software were not properly updated to include a number of key changes in the parameters. Software changes must be adequately documented and communicated to all testing personnel so that both internal validity (programming bugs) and external validity (accuracy of simulation) can be verified. Thorough testing must not yield to schedule pressures, especially during autonomous operations where in-flight errors cannot be remedied by human intervention.

The MIB repeatedly stressed the criticality of independent assessments, audits, and peer reviews throughout the various stages of a mission. It is essential to review the training, experience, and capabilities of the project teams, including contractors. And it is important to confirm that there are sufficiently defined areas of responsibility and that these are communicated across the team. Technical reviews should include examination of raw data and independent testing to verify adequate assessment of project technical risk. Independent reviews provide a system of checks and balances to ensure that the proper safeguards are in place. It is also recommended that project teams formally address and document responses to independent assessments.

Program and project management should regularly review a mission's risk level classification to accommodate for potential shifts in the risk tolerance with changing conditions. Although DART was originally conceived as a low-cost, high-risk demonstration, its significance to NASA grew appreciably over time. But management's risk posture was never re-evaluated or changed. Decisions to change or maintain risk level classifications should be well documented.

The MIB also specifically called for the evaluation of a project's usage of subject matter experts and lessons learned documentation. Program and project teams should fully utilize all of the resources available in order to optimally leverage NASA's past experiences. The DART experience was an example of underutilizing NASA's wealth of expertise, and itself provides important lessons learned for use in future autonomous missions.

Questions for Discussion

- Do you review simulation and testing techniques with the same level of rigor as the test results? Do you periodically ensure that tests are still accurate and applicable for your mission needs?
- Do you have a systems-level understanding of how the outputs of one component may affect the operations of other components?
- Is your project undergoing regular peer reviews or independent assessments of both managerial and technical risks?
- Are all changes officially reported, documented, and tested thoroughly for impacts throughout the system? Even "last minute" changes?
- Are you fully utilizing subject matter experts and NASA's official lessons learned documentation?

References:

Overview of the DART Mishap Investigation Results, NASA, 2006.
http://www.nasa.gov/mission_pages/dart/main/

DART Fact Sheet, Orbital Sciences Corporation, 2004.
http://www.orbital.com/NewsInfo/Publications/DART.pdf

"NASA Launches DART Spacecraft to Demonstrate Automated Rendezvous Capability", NASA, 2005.
http://www.nasa.gov/mission_pages/dart/media/05-049.html

"On Orbit Anomaly Ends DART Mission Early", NASA, 2005.
http://www.nasa.gov/mission_pages/dart/media/05-051.html

"DART Seeks its Target" [Online Image], NASA, 2004.
http://www.nasa.gov/mission_pages/dart/rendezvous/f_dart-tech.html

"DARTing into Space" [Online Image], NASA, 2004.
http://www.nasa.gov/missions/science/dart_into_space.html

DART Spacecraft and Mission, NASA, 2005.
http://www.nasa.gov/mission_pages/dart/spacecraft/index.html

Stover, Dawn. "Battlefield: Space", Popular Science, 10/28/2005.
http://www.popsci.com/military-aviation-space/article/2005-10/battlefield-space

SYSTEM FAILURE CASE STUDIES
A product of the NASA Safety Center

Executive Editor: Steve Wander stephen.m.wander@nasa.gov
Developed by: ARES Corporation

This is an internal NASA safety awareness training document based on information available in the public domain. The findings, proximate causes, and contributing factors identified in this case study do not necessarily represent those of the Agency. Sections of this case study were derived from multiple sources listed under References. *Any misrepresentation or improper use of source material is unintentional.*

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov