The Space Shuttle and GPS – A Safety-Critical Navigation Upgrade

John L. Goodman

United Space Alliance, LLC, 600 Gemini Avenue,
Houston, TX, USA 77058-2777
John.L.Goodman@usa-spaceops.com

Abstract. In 1993, the Space Shuttle Program selected an off-the-shelf Global Positioning System (GPS) receiver to eventually replace the three Tactical Air Navigation units on each space shuttle orbiter. A proven, large production base GPS receiver was believed to be the key to reducing integration, certification, and maintenance costs. More GPS software changes, shuttle flight software changes, and flight and ground testing were required than anticipated. This resulted in a 3-year slip in the shuttle GPS certification date. A close relationship with the GPS vendor, open communication among team members, Independent Verification and Validation of source code, and GPS receiver design insight were keys to successful certification of GPS for operational use by the space shuttle.

1 Introduction

In the early 1990s, Tactical Air Navigation (TACAN) ground stations were scheduled for gradual phase-out starting in the year 2000 due to the introduction of Global Positioning System (GPS) navigation. The five-channel Miniaturized Airborne GPS Receiver (MAGR) was chosen in 1993 to eventually replace the three TACAN units on each shuttle orbiter [1]. A preproduction MAGR (the "3M") flew seven times on Endeavor from December 1993 to May 1996. Test flights of a single MAGR/Shuttle (MAGR/S) began in September of 1996 on STS-79. Certification of the MAGR/S for TACAN replacement and the first all-GPS, no-TACAN flight was scheduled for 1999. By mid-1998, the three TACAN units had been removed from the orbiter Atlantis and three MAGR/S units were installed. However, MAGR/S and shuttle computer issues that surfaced during the flight of STS-91 (June 1998) resulted in a delay in MAGR/S certification. Additional flights and ground tests, along with additional MAGR/S software changes, were mandated. Changes were made to the project to enhance communication among participants, increase insight into the MAGR/S design, and fully integrate the MAGR/S vendor into the project. Three TACAN units were reinstalled in Atlantis and one MAGR/S remained on board for data gathering. By the spring of 2002, all four shuttle orbiters were equipped with one MAGR/S, and certification for TACAN replacement occurred in August of that year. Due to the slip in the

Proceedings of the 2nd International Conference on COTS-Based Software Systems, Ottawa, Canada, February 10-12, 2003. These materials are sponsored by the National Aeronautics and Space Administration under Contract NAS9-20000.

predicted start of TACAN ground station phase-out to 2010 [2], it is expected that the shuttle orbiters will fly with three TACANs and one GPS receiver for some time.

2 Communicate Early, Communicate Often

Cost and schedule concerns can lead to restrictions on communication among both management and technical personnel. Attempts to avoid discussing issues that are "out-of-scope" of the contract can lead to reluctance to discuss topics that are "in scope." Restricting technical discussions to a small group, in the interest of meeting a success-oriented schedule, can result in problems later in the project. This is particularly critical in the requirements definition phase. Requirements and technical issues must be identified and resolved early in a project to avoid negative impact to cost and schedule later in the project [3]. Multiple layers of management and contractors further degrade open, accurate communication, particularly among technical personnel. Lack of communication can lead to misunderstanding of requirements, software design and unit operating procedures, as well as a failure to recognize, properly diagnose, and resolve technical issues. Cost, schedule, and technical problems caused by poor communication may create adversarial relationships at both the organizational and individual levels.

In the wake of the GPS and shuttle computer problems encountered on STS-91, weekly participation in the MAGR/S Problem Resolution Team teleconferences was expanded to include all civil service and contractor organizations on the shuttle GPS team, including the vendor. Face-to-face meetings were held two to four times a year at the Johnson Space Center. Good interpersonal relationships and team building created an environment in which different points of view could be expressed and issues could be resolved in a manner that satisfied the concerns of project members. Special teams that included representatives from various contractor and civil servant organizations were formed to address specific technical issues. Accurate and detailed records of meetings, issues, issue resolution, and design rationale were kept. This allowed participants to stay informed on issues within the project and provided a record for engineers that will work with the MAGR/S in the future.

3 Establish A Close Relationship With The Vendor

Use of software intensive products in high-visibility, high-risk, and safety-related applications requires a higher level of vendor participation than other applications. Many vendors have little or no insight into how their products are integrated and used. The vendor can provide valuable information that should be factored into system and software-level requirements definition, flight and lab testing, issue identification, and issue resolution. Vendor involvement can permit timely identification of problems before cost and schedule are negatively impacted. Advice from the vendor is particularly important if the intended application of the product is significantly different from the application for which it was originally designed.

Integrators and users must maintain enough “in-house” expertise to define integration architecture, perform testing, identify and resolve problems, avoid false diagnosis of healthy units that are perceived to be malfunctioning, define test and operating procedures, and provide management with advice concerning which products are best for an integration. The use of a COTS device should not be used to justify “buying” technical expertise as a COTS product. Vendors in competitive markets may not want key technical personnel assigned to one project for long periods.

Initially, contact with the MAGR/S vendor was limited to a small group of personnel. Information obtained from the vendor was not passed on to other project participants, and the vendor was not consulted enough on integration and performance issues. After STS-91, the MAGR/S vendor was fully integrated into the GPS project team. The vendor was interested in learning how the Space Shuttle Program differed from previous users of their product. Observing shuttle ascent and entry from Mission Control, flying landings in a shuttle simulator, and participating in MAGR/S testing at Space Shuttle Program facilities enabled the vendor to become familiar with the shuttle flight regime, crew and Mission Control procedures, flight rules, and aspects of shuttle mission design. The vendor provided advice that improved ground and flight-testing, issue identification, and issue resolution. Interaction with project participants during weekly teleconferences and face-to-face meetings enabled the vendor to understand concerns and various points of view expressed by project members, enabling them to propose solutions that were agreeable to all parties.

4 Design Insight May Be Necessary

Design insight is required for high-risk, safety-related applications for the COTS integration to be successful. Users of COTS units usually have little or no insight into software design, design rationale, and operation. Available documentation may not contain accurate, pertinent information that would aid an integrator in designing integration architecture, defining interface and software requirements, test and operational procedures, and issue identification and resolution. A vendor supplied Interface Control Document (ICD) may not contain enough information to permit host system interface software requirements creation. Many devices, such as GPS receivers, contain legacy code, some of which may be one or more decades old. Vendor engineers may not have participated in the original development of the product. Over time, “corporate knowledge loss” concerning design rationale occurs due to retirements, employee attrition, office clean-ups, and corporate takeovers. This will make it difficult for the vendor to answer integrator and user questions. Vendor answers to questions may be limited to “how” a device operates, but not “why” it was designed to operate that way. If a vendor is not forthcoming concerning design insight, consultants and other users of the product may be able to provide information.

The STS-91 incident revealed that the shuttle computer software that interfaced with the MAGR/S was designed with an inadequate understanding of MAGR/S operation. The shuttle software was later modified to handle known and unknown receiver anomalies. Expanded vendor involvement after STS-91 brought much needed design insight to the project, which greatly aided issue identification and resolution. In hindsight, some aspects of the MAGR/S interface and integration might have been done differently if the vendor had been involved when the shuttle computer software requirements to support GPS were initially defined.

The vendor provided much needed education concerning the challenges of GPS design and operation in the flight environment for which MAGR was originally designed. A formal "questions for the vendor" list was maintained and answers were recorded.

Insight into test equipment design and operation is critical. Like vendors of GPS receivers, vendors of test equipment may not understand the applications that their equipment supports. Many issues that arose during MAGR/S ground testing concerned GPS signal generators. These issues had an impact on test results, cost, and schedule. Insight into GPS signal generator design and operation was a challenge throughout the project.

5 Define Realistic Schedule, Budget, and Requirements

A key question to be answered is, "Will the proposed use of the product differ greatly from the original application for which it was designed?" This question must be answered in order to create a realistic budget and schedule. If the proposed application is the same or very similar to that for which the product was originally designed, it may be possible to treat it as a "plug and play" project. However, if modifications must be made to accommodate operation in a different environment, the project is really a development project, and a fixed-price contract should be avoided. Fixed-price contracts often result in inflated initial cost estimates and remove the incentive for the vendor to pursue and resolve technical problems.

Technical risk must be taken into account when defining budget and schedule. Traditionally, navigation unit integration has revolved around hardware integration and testing (such as shock, vibration, thermal, radiation). However, with the increasing use of embedded computers, software development, maintenance, and testing must be budgeted for as well.

If extensive modifications and operation in a different environment are required, more testing will have to be performed. Provision for interim software versions should be provided in the budget. The vendor will have to be more involved than on "plug and play” integrations. Understanding the design rationale and original user requirements is important, and provision for discussing this with the vendor should be included.

Lessons learned from users of the same or similar products should be considered, particularly when defining requirements for the COTS item. “Loose” requirements may be easily met with little or no budget impact. However, they could permit problems to go unnoticed and unresolved and could impact future use of the device. Such requirements result in a “let’s see what we can get by with” attitude rather than a “let’s do what is right for the application” approach.

Some GPS receivers used on NASA spacecraft have a specified rate of receiver resets to recover from software anomalies [4] of less than one per day. Such a requirement, along with a maximum allowable solution outage time, will help motivate a vendor to pursue software issues.

6 Plan For Enough Testing and Code Audits

A number of spacecraft failures have resulted from a lack of comprehensive, end-to-end testing [5]. A limited amount of flight and ground testing to ensure that the unit “meets specifications” may not exercise enough of the software to uncover software issues. If the new application is different from that for which the product was designed, and modifications have been made, the amount and scope of testing will have to go beyond that needed to verify that the unit meets contract specifications. Both off-line and integrated testing of interface software in units that interact with the COTS product are required.

The shuttle/GPS integration architecture allowed a single GPS receiver to be flown for data collection while the baseline, certified legacy shuttle navigation system operated. Shuttle software that interfaced with and processed MAGR/S data was exercised in flight. For operational flexibility, shuttle software was designed to support three different vehicle configurations: three TACANs and no GPS, three TACANs and one GPS, or three GPS units and no TACANs.

Flight or lab testing will not find all software issues, nor will it enable verification of all software modifications. GPS signal generators will not exactly duplicate the radio-frequency environment present during a flight, nor will such lab testing exercise all possible logic paths in the GPS receiver software. After STS-91, the role of NASA’s Independent Verification and Validation (IV&V) contractor was expanded to include an audit of the MAGR/S source code, which had been developed at government expense [6]. IV&V personnel possessed prior experience with the MAGR on aircraft integrations. The IV&V contractor played a valuable role in identifying, assessing the criticality of, and assisting with the resolution of software issues. IV&V audits and access to source code may be required for high-risk applications where human safety is a concern. The trend to use non-developmental item products containing proprietary software may be a safety risk in these applications.

Vendors of products such as GPS receivers often state that users do not provide enough data and hardware configuration information when a problem with a unit is reported. The performance of GPS receivers and other software intensive units is a function of a variety of factors. The cause of a suspected software or hardware issue cannot be diagnosed with only position and velocity data. Other parameters characterizing receiver performance should be supplied, in digital form, along with hardware configuration and procedures used. Before contacting the vendor, users should confirm that the suspect performance is not the result of user error.

7 Unrealistic Expectations Lead To COTS Disappointment

The success of inexpensive and easily available GPS technology has led some to believe that applying GPS technology is relatively straightforward, with low risk and low cost. Not understanding the complexity of GPS technology will lead to unrealistic budget, schedule, and technical success expectations. Assuming "cheap and easy" terrestrial GPS means applying such technology to spacecraft will be "cheap and easy" has prevented the maturation of GPS units for use on spacecraft [7].

"COTS disappointment" results from a failure to meet overly optimistic budget and schedule goals (i.e., the number of technical issues encountered exceeded expectations). COTS disappointment will lead to suspicion of the technology in the COTS product and reluctance to work with the technology in the future. The issue is not with "technology," but with unrealistic expectations attached to use of the COTS device. These unrealistic expectations arise from a failure to appropriately investigate and plan for the use of a COTS product when defining schedule, budget, and requirements.

8 Software Quality Is Important

Over the last 40 years, integration of off-the-shelf systems had changed from being primarily hardware integration to software integration. This presents new challenges for users of off-the-shelf systems. Developers of such systems must compete in a market that demands short time-to-market and low overhead. This results in short development and test cycles, less rigorous requirements definition and documentation, and a small group of programmers; and it can lead to a higher probability of software errors. Some products contain "legacy code" that may be decades old, and proper coding standards may not have been adhered to. Vendors often maintain a library of common software modules used in a variety of products. Cost and schedule concerns may lead the vendor, integrator, or user to judge a software issue to be "no impact" and not fix it. However, this can lead to propagation of software problems throughout a product line, and it could negatively impact users whose applications of the product in question are different from the original user.

Historically, navigation unit problems and failures in the legacy shuttle navigation system tended to be of a hardware nature. However, problems encountered with GPS have concerned software. GPS receivers contain tens or hundreds of thousands of lines of code. Code errors may not always manifest in a predictable or easily observable manner and may lie dormant for years until the proper set of conditions permits them to become visible. Software errors that do not manifest in an aircraft application of a GPS receiver may be an impact in orbit, where vehicle dynamics, satellite visibility, and flight times are very different.

Much attention has been paid to detecting and mitigating the impact of GPS satellite malfunctions on GPS receivers through the use of ground station monitoring (such as the U.S. Wide Area Augmentation System or the European Geostationary Navigation Overlay System) or suspect measurement detection and isolation (Receiver Autonomous Integrity Monitoring) within the receiver itself. A recent study [8] of stand-alone aviation GPS receivers that meet Federal Aviation Administration TSO C-129 requirements found that the probability of a receiver outage from a software issue was higher than a signal in space problem from a malfunctioning GPS satellite. The study concluded that more attention should be paid to improving GPS receiver software quality and characterizing GPS receiver failure probability and failure modes. Test flights of GPS receivers on the space shuttle have led shuttle navigation personnel to the same conclusions.

9 Provide Guidelines for COTS Use and Application of Faster-Better-Cheaper Principles

Recent analyses indicate that a lack of guidance on the application of COTS and faster-better-cheaper principles leads to projects that exceed cost and schedule estimates, and, in some cases, resulted in project failure [9, 10]. Policies governing COTS and faster-better-cheaper approaches must be defined to permit clear and consistent application and to mitigate risk to budget and schedule [11-19].

Trade studies of COTS products involving "must meet," "highly desirable," and "nice to have" requirements will help determine what product to choose, what requirements it must meet, and if a custom approach should be taken instead. Any addition to or relaxation of requirements must be identified. A need for new requirements may not become visible until testing and implementation of the product is underway. The impact of COTS driven hardware and software changes to an integrated system must be assessed.

A certification plan must take into account how much vendor certification can be relied on and if additional testing beyond what the vendor performs is needed. Vendor certification for both hardware and software should be studied to determine if it is adequate. Vendor support required for testing, integration, and maintenance over the life cycle of the product must be defined. If white box testing (rather than black box testing) must be performed, design insight from the vendor will be required and proprietary agreements must be negotiated. The vendor may possess information on problems other users have encountered, which will be useful during integration and over the life cycle of the product.

Guidelines for use of COTS or Modified Off-The-Shelf (MOTS) software based on the criticality of the application in question were developed by the Space Shuttle Program in the wake of the GPS integration effort [20].

10 Summary

The Space Shuttle Program has successfully integrated and certified an off-the-shelf GPS receiver into the space shuttle avionics system. However, the time and effort required to certify the integration exceeded expectations. Integration and use of software intensive, off-the-shelf units into safety-related applications for which they were not originally designed requires vendor support and design insight above that required for other off-the-shelf integrations.

References

1. Goodman, John L.: Space Shuttle Navigation In The GPS Era. In: Proceedings of the National Technical Meeting 2001. Institute Of Navigation, Fairfax, VA (January 22-24, 2001) 709-724
2. Federal Radionavigation Plan – 2001. U. S. Departments of Defense and Transportation. (2002)
3. Rosenberg, Dr. Linda H., et al.: Generating High Quality Requirements. AIAA Paper 2001-4524. In: Proceedings of the AIAA Space 2001 Conference and Exposition. American Institute of Aeronautics and Astronautics, Reston, VA (August 28 to 30, 2001)
4. Bertiger, Willy, et al.: Precise Orbit Determination For The Shuttle Radar Topography Mission Using A New Generation Of GPS Receiver. In: Proceedings of ION GPS 2000. Institute of Navigation, Fairfax, VA (September 19-22, 2000)
5. Newman, J. Steven: Failure-Space: A Systems Engineering Look At 50 Space System Failures. Acta Astronautica, Elsevier Science Ltd, Volume 48, Numbers 5-12 (2001) 517-527
6. Beims, M. A., and J. B. Dabney: Reliable Tailored-COTS Via Independent Verification and Validation. In: Proceedings of NATO Commercial Off-The-Shelf Products in Defense Applications Symposium. Brussels, Belgium (April 3-7, 2000)
7. Bauer, Frank H., et al.: Spaceborne GPS Current Status and Future Visions. In: Proceedings of ION GPS-98. Institute Of Navigation, Fairfax, VA (September 15-18, 1998) 1493-1508
8. Nisner, P. D., and R. Johannessen: Ten Million Data Points From TSO Approved Aviation GPS Receivers: Results of Analysis and Applications to Design and Use in Aviation. In: Navigation: Journal of the Institute of Navigation, Vol. 47, No. 1. Institute Of Navigation, Fairfax, VA (Spring 2000) 43-50

9. Anderson, Christine, et al.: Lewis Spacecraft Mission Failure Investigation Board Final Report. (February 12, 1998)
10. Gross, Roberta L.: Faster, Better, Cheaper: Policy, Strategic Planning, And Human Resource Alignment. NASA Office Of The Inspector General. Report Number IG-01-009 (March 13, 2001)
11. Adams, Richard J. and Suellen Eslinger: Lessons Learned From Using COTS Software on Space Systems. In: Crosstalk - The Journal Of Defense Software Engineering. U.S. Department of Defense (June 2001)
12. Brownsword, Lisa, David Carney and Tricia Oberndorf: The Opportunities and Complexities of Applying Commercial-Off-the-Shelf Components. In: Crosstalk - The Journal Of Defense Software Engineering, U.S. Department of Defense (April 1998)
13. Carney, David J. and Patricia A. Oberndorf: OSD - Commandments of COTS: In Search of the Promised Land. In: Crosstalk - The Journal Of Defense Software Engineering, U.S. Department of Defense (May 1997)
14. Carney, David: Quotations From Chairman David – A Little Red Book Of Truths To Enlighten And Guide On The Long March Toward The COTS Revolution. Carnegie Mellon University Software Engineering Institute, Pittsburgh, PA (1998)
15. Dean, J., and A. Gravel (editors): COTS-Based Software Systems. In: Proceedings of the First International Conference on COTS-Based Software Systems (ICCBSS 2002). Lecture Notes in Computer Science Series, Volume 2255. Springer-Verlag, Heidelberg, Germany (2002)
16. Lipson, Howard F., Nancy R. Mead and Andrew P. Moore: Can We Ever Build Survivable Systems from COTS Components? CMU/SEI-2001-TN-030. Carnegie Mellon Software Engineering Institute, Pittsburgh, PA (December 2001)
17. Meyers, B. Craig and Patricia Oberndorf, Managing Software Acquisition: Open Systems and COTS Products. In: The SEI Series in Software Engineering, ISBN 0-201-70454-4. Addison-Wesley, Boston, MA (2001)
18. Oberndorf, Patricia: COTS and Open Systems. Carnegie Mellon University Software Engineering Institute, Pittsburgh, PA (February 1998)
19. Place, Patrick R. H.: Guidance on Commercial-Based and Open Systems for Program Managers. CMU/SEI-2001-SR-008. Carnegie Mellon Software Engineering Institute, Pittsburgh, PA (April 2001)
20. Dittemore, Ronald D.: Commercial Off-the-Shelf (COTS), Modified Off-the-Shelf (MOTS) Software Policy. SSP Directive No. 145, Dated April 16, 2001. In: Space Shuttle Program Structure And Responsibilities, Book 2, Space Shuttle Program Directives, NSTS 07700. NASA Johnson Space Center.