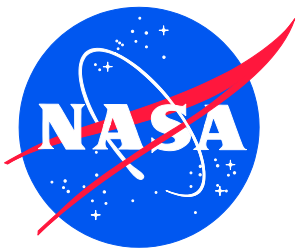
NASA/TP–20230005922
NESC-TP-22-01762



Best Practices for the Design, Development, and Operation of Robust and Reliable Space Vehicle Guidance, Navigation, and Control Systems

Cornelius J. Dennehy/NESC
Langley Research Center, Hampton, Virginia

April 2023

NASA STI Program Report Series

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

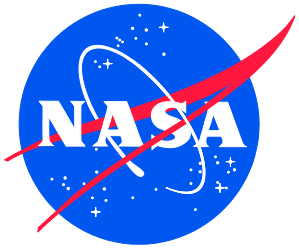
For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- Help desk contact information:

https://www.sti.nasa.gov/sti-contact-form/
and select the "General" help request type.

NASA/TP–20230005922
NESC-RP-22-01762



Best Practices for the Design, Development, and Operation of Robust and Reliable Space Vehicle Guidance, Navigation, and Control Systems

Cornelius J. Dennehy/NESC
Langley Research Center, Hampton, Virginia

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

April 2023

Acknowledgments

The results documented in this report were produced with the support of and from technical interactions with several individuals from the NESC and other organizations. The author would like to thank and acknowledge the significant technical contributions of Aron Wolf, Tannen VanZwieten, Kenneth Lebsock, John West, James Blue, Michael Cleary, Jerold Gilmore, Bruce Jackson, Scott Miller, Mike Bay, Mitch Davis, Mike Aguilar, Dorre Poppe, Jeb Orr, Davin Swanson, Gary Henderson, Oscar Alvarez-Salazar, Russell Carpenter, Chris D'Souza, John Osborne, Tim Barth, and Daria Topousis. James Miller and Christina Cooper at NASA/LaRC are acknowledged for their assistance in editing and refining our original NESC GN&C Best Practices report in 2007. Special thanks to Oscar Gonzalez, Brett Starr, and Uday Shankar for their peer review of the preface. Jenny DeVasher at NASA/LaRC is to be acknowledged for her efforts as technical editor on this updated NASA Technical Publication.

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

Preface

Introduction

The NASA Engineering and Safety Center (NESC) completed, in 2007, an in-depth assessment to identify, define, and document engineering considerations for the design, development, and operations of human-rated spacecraft systems [ref. 1].[1] The assessment was requested by the Astronaut Office at NASA's Johnson Space Center (JSC) to help provide an in-depth understanding of what is required to ensure reliable, robust, and safe human-rated spacecraft systems. Experts in reliability, discipline-specific subject matter, and systems engineering were brought together to synthesize the current best practices, sometimes referred to as "preferred practices," at the spacecraft system and subsystem levels.

The Guidance, Navigation, and Control (GN&C) system is a fundamental element of most, if not all, crewed and robotics space vehicles. Thus, one of the major sections of the 2007 report (specifically, Section 7) focused on design considerations for GN&C systems for spacecraft. In addition to examining the GN&C legacy for crewed spacecraft, the 2007 NESC assessment team also studied GN&C engineering lessons learned from several robotic spacecraft mishaps and failures. In the process of conducting the 2007 assessment, the team concluded that the engineering best practices identified from the study of robotic spacecraft experiences also applied directly to the design, development, and operations of GN&C subsystems for human-rated launch vehicles and spacecraft. Now in 2023, it has become even more clear that with the passage of over 15 years there is a tremendous overlap and commonality between GN&C engineering best practices for crewed and robotic space vehicles.

Critical Need to Share GN&C Best Practices and Lessons Learned

With an unprecedented level of space system development activities ongoing at NASA and our industry partners, a critical need exists to communicate and more broadly share with the NASA GN&C Engineering Community of Practice (CoP) the basic set of best practices developed in 2007 and updated herein.

Without question, NASA needs a well-defined set of engineering design guidelines and best practices for implementing reliable and robust GN&C spacecraft systems, which is the fundamental purpose of this publication. NASA has recognized that it must improve its process for identifying, documenting, and sharing lessons learned from development, flight, or research projects [ref. 45]. The first attempt to more widely share these GN&C engineering considerations was accomplished in 2007 with the publication of an AIAA paper titled *"GN&C Engineering Best Practices For Human-Rated Spacecraft Systems"* [ref. 2]. That paper provided a high-level summary of GN&C best practices from the 2007 NESC report.

The objective of this NASA Technical Publication is to comprehensively capture and more widely disseminate the GN&C design best practices identified during the 2007 NESC assessment. This publication documents, in a standalone reference, the specific GN&C-related results of the original assessment. The fundamental intent is to improve the GN&C system design, development, and operations process within NASA and with our industry partners. The

[1] Please note that, unless otherwise stated, the references called out in this Preface are from Section 2.1, Additional Post-2007 References.

creation, review, and wide dissemination of this report is absolutely consistent with the NESC's commitment to achieving engineering excellence by capturing and passing along to the next generation of engineers the lessons learned from the collective professional experiences of GN&C subject matter experts.

This report will not only provide relevant guidance for early-career GN&C engineers, but also serve as a useful memory aid for more experienced engineers, especially as a reference for technical peer reviews of GN&C systems under development.

Report Scope

This report includes the complete original GN&C information and findings that emerged from the 2007 NESC assessment. In particular, this report attempts to harmonize GN&C engineering best practices for crewed and robotic spacecraft. This report will provide the reader with:

1. A brief introduction to GN&C system engineering.
2. The driving GN&C interactions and interdependencies with other spacecraft systems.
3. High-level description of the GN&C design, development, and operations process.
4. Discussion of GN&C robustness, reliability, and fault tolerance issues as illustrated by the history of crewed and robotic GN&C missions.
5. Some historical background highlighting the Gemini, Apollo, and Shuttle GN&C systems for crewed-mission context.
6. Specific engineering best practices that yield a robust and reliable GN&C subsystem.

Wherever possible, relevant linkages are established between the best practices and specific lessons learned from past space mission failures and mishaps.

A total of 22 GN&C engineering best practices are described in this report, ranging from fundamental system architectural considerations to more specific aspects (e.g., stability margin recommendations) of system design and development. As the reader will see, the first 15 apply principally to early GN&C engineering work associated with "Architecting the Right System." The remaining seven apply to the later stages of the GN&C design, development, and operations process, mostly focused on the end goal of "Building the System Right."

For a more complete space vehicle perspective, readers should review the two-volume 2007 NESC assessment report [ref. 1] to understand some of the critical lessons learned and best practices from other engineering disciplines, such as avionics, software, mechanisms, and propulsion, that typically interact and interface with a spacecraft's GN&C system.

Understanding and Applying the GN&C Best Practices

Perhaps surprisingly, the 22 best practices documented in this report are generally applicable to missions across the broad spectrum of NASA's science and exploration mission portfolio. However, it should be understood that the set of NESC GN&C Best Practices from 2007 documented in this report will not be applicable as-is to all project and mission applications. Some tailoring is to be expected in the process of applying these practices. Prior to using these best practices, the reader must have a clear understanding of mission goal(s) as well as be able to assess impacts of the risk posture(s), expected mission environment(s), expected application(s)

and expected mission life. These key elements will set the boundaries and basis for specific mission-unique GN&C design and development steps. Understanding these elements will help the reader ascertain which lessons and/or best practices the GN&C design team should focus on and which may need to be further verified (e.g., environmental conditions, life, redundancy implementation).

Key Guiding Principles

Many of the following points will be addressed in detail in this report, but it may be useful to reiterate here for the reader some of the guiding GN&C system engineering principles that emerged from the 2007 assessment:

1. **Have a solid understanding of overall mission requirements.** Obtain a clear and simple set of prioritized program needs, goals, objectives, and constraints that will form the basis of GN&C design and development work. Identify the high-level governing documents that specify relevant NASA Procedural Requirements (NPRs) for the mission. Assess the GN&C design and development impacts of complying with these NPRs. Understand the mission risk classification and its impact on GN&C design and development.
2. **Early on, establish the management organization with related responsibilities and project lines of authority.** Manage and lead the GN&C team with simple and easy-to-understand organizational structures, clear lines of authority, and well-defined roles, responsibilities, and interfaces across the various team elements.
3. **Specify safety and reliability requirements through a triad of fault tolerance, bounding failure probability, and adherence to proven engineering practices and standards**. The mission's risk posture (i.e., risk tolerance) will strongly influence this aspect of the early GN&C work.
4. **Be intellectually curious and proactive in anticipating potential system failure modes and anomalistic behaviors.** Do not let the design suffer from team member overconfidence or complacency, which can result in a lack of imagination in the process of envisioning previously unknown failure modes, investigating system limitations and weaknesses, and exploring possible recovery paths. Instead, have a healthy skepticism about the GN&C system and strive to expect the unexpected. Resist the temptation of assumming that past success will automatically translate to the future. Do not rely exclusively on past lessons learned to postulate potential failure modes in the new system. Consider the use of "pre-mortem" analyses and evaluations to anticipate and prepare for potential GN&C system failure modes and anomalistic behaviors.
5. **Be aware of the curse of complexity.** Thoughtfully manage GN&C system complexity by keeping primary mission objectives as simple and minimal as possible and adding complexity to the system only where necessary to achieve these objectives. Be aware that as GN&C system complexity grows, so does the associated spacecraft flight software (FSW) complexity, which can lead to challenges in managing flight operations and knowing exactly what to do in off-nominal mission events.
6. **Spend sufficient time early in the mission formulation phase to synthesize a robust system architecture consistent with mission goals, requirements, constraints, and risk posture.** An inferior GN&C architecture can be brittle, with few robustness qualities.

Desirable GN&C architectures allow for growth in the mission set and have high measures of effectiveness, safety, reliability, affordability, and sustainability. A superior architecture for most spacecraft GN&C subsystems typically emerges from multiple face-to-face iterations between the architects/designers and stakeholders/customers/end users. Coordinating and directing those iterative interactions and ensuring they occur early and converge soon enough to facilitate management decisions is an important responsibility of the GN&C system engineer (SE). Lastly, one cautionary note: One should guard against the tendency to be too flexible with the GN&C system architecture. Don't allow changes in the baseline architecture to be freely made without fully evaluating the consequences with sufficent trade study analysis.

7. **Formulate the space vehicle's GN&C requirements with care and thoughtfulness.** Keep in mind that the requirements serve as a means of coordination across the project team and ensure the accomplishment of mission objectives. Consider that a proper set of requirements will provide an unambiguous, tangible, and quantitative framework for the entire GN&C team to work toward. Unlike mission objectives, the requirements can be tailored, adjusted, or even eliminated to achieve mission objectives, subject to the applied constraints. It is imperative to be aware that each requirement has a direct and indirect cost. Sufficient trade study work is necessary to converge on a cost estimate for each requirement. A revealing exercise is to weigh the total cost of each requirement against its individual contribution to meeting the mission objectives.[2] It is good practice to document the rationale for each GN&C requirement for later traceability back to mission objectives. Avoid the case where requirements are simply taken from a previous mission and blindly applied to the mission at hand without adequate review and consideration of their relevance.
8. **Conceive the right system conceptual design early in the life cycle.** Thoroughly explore risks from the top down and use a risk-based design approach to iterate the operations concept, design, and requirements until the system meets mission objectives at minimum complexity and is achievable within constraints.[3]
9. **Seek out and fully utilize independent GN&C subject matter experts.** These are individuals with in-depth knowledge and experience who are not involved in the GN&C design and development effort under consideration and are willing to provide critical technical insights and assistance. Engaging with such experts will allow the GN&C team to benefit from the experience of others. Implementing an engineering peer review process for technically complex missions is a prudent and proactive step. The project's GN&C team should be required to formally address and document its disposition of peer reviewers' findings and recommendations.
10. **Implement a rigorous approach to GN&C-level risk management consistent with the mission's risk classification.** Seek and collect warning signs and precursors to safety,

---

[2] These cautionary observations on requirements and their cost were inspired by technical interactions with both T.K Mattingly and Bass Redd (both from NASA JSC) on the lessons they learned from the real world.

[3] A detailed discussion of the risk-based system design approach, and how it can be used to drive a safe and reliable system with minimum complexity, is provided in Section 2.3.3 in Volume I of the original 2007 NESC assessment final report [ref. 1].

mission success, and developmental risk throughout the life cycle and integrate those into a total risk picture with appropriate mitigation activities. Continuously re-evaluate risks and associated risk mitigations. Strongly advocate for the application of the project's financial reserves to buy down, early on, GN&C technical risks when merited (in-flight FSW algorithm code modifiactions and parameter updates cannot be expected to fix everything).

11. **Do not underestimate the challenges of performing adequate verification and validation (V&V).** Planning for V&V testing should start early in the mission life cycle. V&V testing and analysis is an expensive endeavor and can consume more time and resources than the design phase of a mission. This is especially true for complex GN&C systems. Be aware of the potential for verification gaps due to increased system complexity relative to previous missions. In the development of a V&V testing program, the GN&C SE should be guided by the "Test As You Fly" maxim. This approach includes critical examination where such testing is not possible or is accomplished in pieces to ensure sufficient test coverage in expected flight environments and operational sequences. More so than for other spacecraft subsystems, it can be difficult to "Test As You Fly" for GN&C systems [ref. 46]. GN&C system testing to scale and to environment is severely constrained by the 1-g ground test environment. The GN&C V&V process, therefore, places extraordinary reliance upon modeling and simulation. It typically requires the use of rigorous high-fidelity models, not simplified representations. Modeling assumptions, limitations, and uncertainties should be well understood and documented. Models and simulations need to be independently validated. Clear plans and procedures for certifying all GN&C V&V testbeds and test environments should be established.
12. **Apply a multilayered "defense in depth" approach by following proven design and manufacturing practices, holding independent reviews, inspecting the end product, and employing a "test as you fly, fly as you test" philosophy.** Flight history has shown us that there is no component, subsystem, or system completely free from potential failure and/or anomalistic behaviors. Ensuring safety and reliability in a complex system operating in uncertain environments argues for overlapping and diverse methods to not only develop the system properly, but also provide maximum coverage for identifying and screening potential problems. No single layer will function perfectly in producing a safe and reliable system. All the layers are needed to synergistically provide the opportunity and coverage necessary to ensure details have been adequately considered. A multilayered approach, as shown in Figure 1 below, has been proven successful in developing space systems to function as intended and required and also allowing the discovery of potential catastrophic problems [ref. 1, vol. 1, Executive Summary].
13. **Employ a "Fly As You Test" approach during the flight operations mission phase.** This limits the chance of encountering an unexpected interaction among system elements and their environments not previously explored during verification testing.
14. **Ensure that sufficently detailed GN&C documentation is created and configuration controlled at all steps of the system design and development process.** In particular, all assumptions should be well-documented. It is a best practice to document early in the design and development process the GN&C coordinate frames and system of units to be employed. Lastly, obtaining suffcient supporting documentation from the GN&C component vendors is also a critical need.

15. **Consider, during the design and development stages, any potential GN&C requirements for the support of End-of-Mission disposal functions and operations.** This activity is also known as End-of-Life disposal, decommissioning, controlled reentry, or simply disposal. Often such requirements exist for robotic spacecraft in Low Earth Orbit (LEO) and Geosynchronous Earth Orbit (GEO). Many robotic spacecraft in these orbital regimes must, per international guidelines, be properly disposed of to limit the growth of orbital debris and better preserve orbital environments for future missions. Looking back, we see that the 2007 NESC assessment did not formulate specific GN&C best practices for the End-of-Mission disposal phase. In the future, the NESC may consider updating the 2007 set of GN&C best practices to leverage the design, development, and operational lessons learned from NASA's experiences with spacecraft disposal.

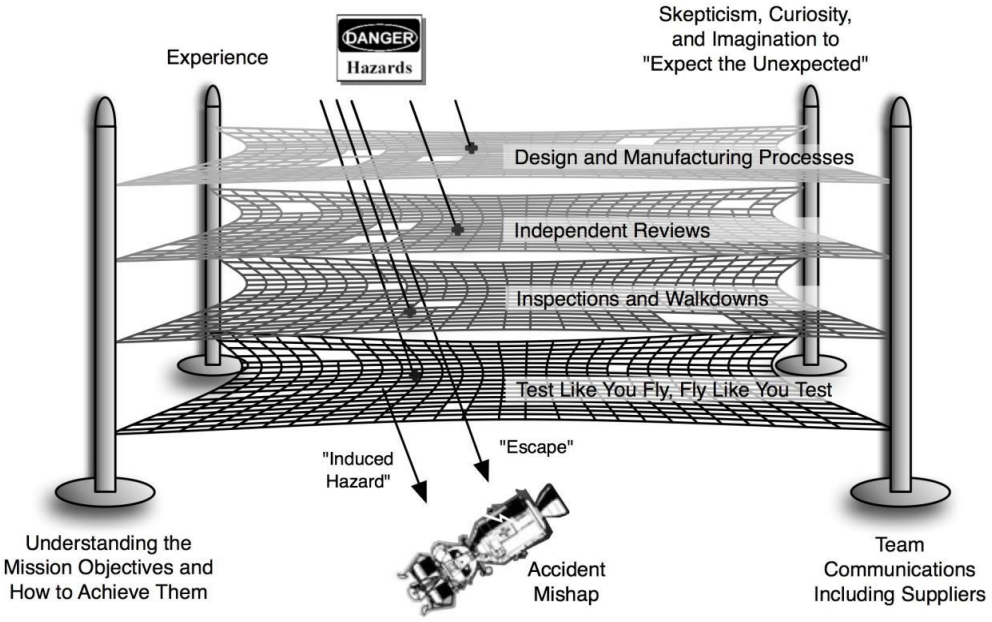


Figure 1. Multilayered Approach Produces a Reliable System

One final thought about GN&C system complexity: When mission needs (e.g., GN&C performance requirements) are pushed to the limit, complexity emerges as a key system design consideration. Complexity and reliability are in direct opposition. Addressing the challenge of discovering system unknowns means ensuring that complex systems are testable and verifiable prior to flight. Thus, complexity should be limited to what is needed to accomplish the mission such that the outcome is a testable GN&C system design.

Post-2007 Activities Relevant to GN&C Best Practices

Since the 2007 NESC assessment covering design, development, and operations engineering best practices for human-rated spacecraft systems, several other studies and analyses (many, but not all, sponsored by the NESC) have focused on GN&C system lessons learned and best practices, GN&C V&V challenges, GN&C technology challenges, and the strong trend towards employing higher levels of GN&C system autonomy. The results of these related post-2007 activities are listed in Section 2.1 as additional new references [refs. 4–29]. I strongly recommend the reader

examine these references for their positive practical value. One that I particularly want to highlight is the NESC's Navigation Filter Best Practices assessment report, published in 2018 [ref. 21]. This useful document succinctly captures 50 years of NASA experience in making design choices for spacecraft onboard navigation filters.

Otto von Bismarck, the man credited with creating the modern German state, is known to have said *"Only a fool learns from his own mistakes. The wise man learns from the mistakes of others."* With this sentiment in mind, it is informative and potentially insightful to momentarily step back from a narrow focus on the GN&C subsystem and consider, from a historical perspective, the broader fundamental, systemic, and underlying issues that have led to past failures and mishaps at NASA. To this end, the NESC completed an assessment in 2020 that looked into the recurring causes underlying human spaceflight mishaps during flight tests and the early operational phase [ref. 29]. Eight mishaps from the Apollo, Soyuz, Skylab, Space Shuttle, and Constellation Programs (i.e., the Ares-1X test flight) and commercial suborbital systems were included in the study. As documented, the nine most frequently recurring causes of the failures and mishaps studied by the NESC were:

1. **Inadequate technical controls or technical risk management practices** (e.g., inadequate readiness reviews, technical issues, or safety hazards not sufficiently analyzed with failure modes and effects analyses (FMEAs), process FMEAs, hazard reports, risk analyses, and similar methods, and inadequate aggregation of incremental technical risks).
2. **Incomplete procedures** (e.g., missing steps; situations or scenarios not adequately covered by written procedures).
3. **System design and development issues** (e.g., testing, human-system integration, material selection, and modeling and simulation issues).
4. **Inadequate inspection or secondary verification requirements** (e.g., missing or deficient requirements; requirements based on incorrect assumptions).
5. **Inadequate organizational learning systems** (e.g., unlearned lessons within or outside human spaceflight organizations).
6. **Inadequate schedule controls** (e.g., unrealistic schedule goals; lack of schedule coordination).
7. **Inadequate task analysis and design processes** (e.g., missing or deficient task analyses; emergency/contingency procedure issues).
8. **Organizational design issues** (fragmented organizations; organizations with unclear accountability for integration functions).
9. **Organizational safety culture issues** (e.g., complacency and competing internal cultures).

Several of these causes should resonate with those of us within the GN&C CoP, regardless of whether we are working on GN&C systems for crewed or robotic spacecraft. Key examples include technical issues not sufficiently analyzed with failure modes and effects analyses, modeling and simulation issues, missing or deficient requirements, requirements based on incorrect assumptions, inadequate organizational learning systems, unlearned lessons, and complacency. We should be ever mindful of these underlying issues as we go about our GN&C design and development work.

Final Thoughts and Observations

In closing, let me emphasize what we all know but perhaps lose sight of in the face of cost, schedule, and other pressures and constraints:

> ***As NASA's spacecraft designers, we are all personally responsible for developing safe, robust, resilient, and reliable spacecraft for performing demanding robotic and human space exploration missions.***

The significant investment of NASA resources for implementing these space systems requires us all to strive to meet high standards of reliability and mission success. The designers and developers of GN&C systems for NASA's spacecraft must, like our colleagues in the other engineering disciplines, be fully committed to this goal. Among our scientists and human exploration architects, the trend to continually push space system engineers to provide higher levels of performance while operating in uncertain, and in some cases unknown, environments only heightens the challenge. From the admittedly rather narrow viewpoint of regarding GN&C as a standalone engineering discipline, we see an exceptional historical success rate of spacecraft GN&C system designers and developers. And while this is true, we all must remain vigilant and strongly resist complacency in our day-to-day engineering activities.

While we surely are personally responsible for, and should take ownership of, developing safe, robust, and reliable spacecraft, we are not working alone. In a talk given more than 45 years ago [ref. 3], astronaut Deke Slayton delivered a powerful message emphasizing the point that mission success depends on everyone on the team being engaged in the design and development process:

> *"Crew safety is not a discrete function performed by specialists at a specific time and place in a program. It is embodied in the total efforts of everyone involved in a project, from concept through completion. … Mission success and crew safety carry almost identical definitions in manned spaceflight."*

The expectation is that the GN&C best practices documented in this report will evolve and be refined over time. Flight experiences, refinements in engineering practices/tools, and technology advances will all shape this evolution. I encourage the NESC GN&C Technical Discipline Team (TDT) to continue to update this list, and for individuals from within the GN&C CoP to submit new GN&C lessons learned and recommended best practices to the NESC.

Reader feedback on this report in general, as well as readers' specific comments and recommendations on how to improve the GN&C engineering CoP at NASA, will be most welcomed by the NESC, most of all by the NASA Technical Fellow for GN&C. In particular, I encourage the members of our GN&C CoP to be as open and candid as possible in communicating and documenting their individual experiences and lessons learned. We all share the responsibility to provide future GN&C teams with technical advice that can increase their effectiveness and efficiency and build on the experiences of our hard-working CoP.

Cornelius J. Dennehy
NASA Technical Fellow for GN&C
March 2023
Greenbelt, Maryland USA

Table of Contents

List of Figures

List of Tables

Acronyms and Nomenclature

2GRLV	Second Generation Reusable Launch Vehicle
AACS	Attitude and Articulation Control Subsystem
ACRIMSat	Active Cavity Radiometer Irradiance Monitor Satellite
ACS	Attitude Control Subsystem
AFRL	Air Force Research Laboratory
AGS	Ascent Guidance Software
AIAA	American Institute of Aeronautics and Astronautics
AKM	Apogee Kick Motor
AMD	Angular Momentum Desaturation
AMR	Assurance Management Representative
APAS	Androgynous Peripheral Attach System
APCS	Attitude Pointing and Control System
AR&D	Autonomous Rendezvous and Docking
ARCSS	Autonomous Rendezvous and Capture Sensor System
ASTP	Apollo-Soyuz Test Project
ATM	Apollo Telescope Mount
ATV	Automated Transfer Vehicle
AVGS	Advanced Video Guidance Sensor
BIT	Built-In Test
BITE	Built-In Test Equipment
CAM	Collision Avoidance Maneuver
CCP	Commercial Crew Program
CCS	Computer Command Subsystem
CDR	Critical Design Review
CDS	Command and Data Subsystem
CM	Command Module
CMG	Control Moment Gyroscope
CONTOUR	Comet Nucleus Tour
CoP	Community of Practice
CSI	Controls-Structures Interaction
CSM	Command Service Module
CTV	Compatibility Test Vans
DARPA	Defense Advanced Research Projects Agency
DART	Demonstration of Autonomous Rendezvous Technology
DDT&E	Design, Development, Test, and Evaluation
°/s	Degrees per Second

DEL	Data Evaluation Lab
DMSP	Defense Meteorological Satellite Program
DoD	Department of Defense
DoF	Degrees of Freedom
DR	Discrepancy Reports
EDL	Entry, Descent, and Landing
EGI	Embedded GPS/INS
EGNOS	European Geostationary Navigation Overlay System
EM	Engineering Model
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESA	European Space Agency
EU	Engineering Unit
EVA	Extravehicular Activity
FBC	Faster, Better, Cheaper
FDIR	Fault Detection, Isolation, and Recovery
FEM	Finite Element Model
FIB	Failure Investigation Board
FMEA	Failure Modes and Effects Analysis
FO	Fail Operational
FOT	Flight Operations Team
FOV	Field of View
FPGA	Field Programmable Gate Array
FSW	Flight Software
GDS	Ground Data System
GFO	GEOSAT Follow-On
GLONASS	Global Navigation Satellite System
GN	Ground Network
GN&C	Guidance, Navigation, and Control
GPS	Global Positioning System
GPSR	Global Positioning System Receiver
GSE	Ground Support Equipment
HAINS	High Accuracy Inertial Navigation System
HAPS	Hydrazine Auxiliary Propulsion System
HITL	Hardware-in-the-Loop
HTV	H-II Transfer Vehicle
HXLV	Hyper-X Launch Vehicle

HXRV	Hyper-X Research Vehicle
I&T	Integration and Test
ICD	Interface Control Document
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
IPT	Initial Power-on Test
IRU	Inertial Reference Unit
ISS	International Space Station
IV&V	Independent V&V
JAXA	Japan Aerospace Exploration Agency
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
kg	Kilogram
km	Kilometer
L/D	Lift Over Drag
lbf	foot-pound
LEO	Low Earth Orbit
LIDS	Low-Impact Docking System
LLIS	Lessons Learned Information System
LM	Lunar Module
LTM	Loop Transfer Matrix
MACS	Modular Attitude Control System
MAGR	Miniaturized Airborne GPS Receiver
MAGR/S	MAGR/Shuttle
MCC	Mission Control Center
MCO	Mars Climate Orbiter
MCS	Motion Control System
MDM	Multiplexer/Demultiplexer
MER	Mars Exploration Rover
MGS	Mars Global Surveyor
MIB	Mishap Investigation Board
MIMO	Multiple-Input/Multiple-Output
MIT-IL	Massachusetts Institute of Technology–Instrumentation Laboratory
MMH	Monomethyl Hydrazine
MO	Mars Observer
MO&DSD	Mission Operations and Data Systems Directorate
MOC	Mission Operations Center

MOCC	Mission Operations Control Center
MODIS	Moderate Resolution Imaging Spectroradiometer
MOI	Mars Orbit Insertion
MPF	Mars Pathfinder
MPL	Mars Polar Lander
MSU	Monitoring and Safing Unit
MTBF	Mean Time Between Failure
MUBLCOM	Multiple Paths, Beyond-Line-of-Sight Communications
MUF	Model Uncertainty Factor
NASCOM	NASA Communications
NASDA	National Space Development Agency of Japan (now JAXA)
NEAR	Near Earth Asteroid Rendezvous
NPR	NASA Program Requirements
NRA	NASA Research Announcement
NTO	Nitrogen Tetroxide
OAE	Orbit Adjust Engine
OAMS	Orbit and Attitude Maneuvering System
OBC	Onboard Computer
OMS	Orbit Mode Software
OSC	Orbital Sciences Corporation
PDF	Programmable Data Formatter
PIT	Pre-Installation Test
PMD	Propellant Management Device
POR	Power-On Reset
ppm	Parts per Million
RCS	Reaction Control System
REA	Reaction Engine Assembly
RF	Radio Frequency
RLG	Ring Laser Gyroscope
RM	Redundancy Management
RMS	Remote Manipulator System
ROS	Russian Orbital Segment
RPA	Radio Power Amplifier
rpm	Revolutions per Minute
RPOP	Rendezvous and Proximity Operations Program
RR	Rendezvous Radar
RSA	Russian Space Agency

RVR	RendezVous laser Radar
RWA	Reaction Wheel Assembly
SAIL	Shuttle Avionics Integration Laboratory
SDF	Single Degree of Freedom
SDO	Solar Dynamics Observatory
SE	Systems Engineer
SF	Scale Factor
SIGI	Space Integrated GPS/Inertial Navigation System
SISO	Single Input-Single Output
SM	Service Module
SMEX	Small Explorers
SMM	Solar Maximum Mission
SMS	Shuttle Motion Simulator
SN	Space Network
SOC	Simulations Operations Center
SRM	Solid Rocket Motor
SSTI	Small Satellite Technology Initiative
STEDI	Student Explorer Demonstration Initiative
STS	Space Transportation System
TACAN	Tactical Area Navigation
TCM	Trajectory Correction Maneuver
TDRSS	Tracking & Data Relay Satellite System
TDT	Technical Discipline Team
TIROS	Television Infrared Observation Satellite
TOMS	Total Ozone Mapping Spectrometer
TOMS-EP	TOMS-Earth Probe
TRL	Technology Readiness Level
TRW	Thompson Ramo Wooldridge
TSO	Technical Standard Order
TVC	Thrust Vector Control
U.S.	United States
UARS	Upper Atmospheric Research Satellite
V&V	Verification and Validation
VAFB	Vandenberg Air Force Base
WAAS	Wide Area Augmentation System
WIRE	Wide-Field Infrared Explorer
XSS-11	Experimental Satellite System-11

Abstract

This document summarizes and updates the NESC Guidance, Navigation, and Control (GN&C) Technical Discipline Team's (TDT) work to synthesize and document the current best practices for the design & development of robust and reliable GN&C systems for robotic and crewed (human-rated) spacecraft. These GN&C best practices for future science and exploration missions were derived from the lessons learned, both positive and negative, on earlier spaceflight projects, both robotic and crewed. An attempt has been made to capture preferred practices that reflect the key considerations, trades, and processes directly attributed to past mission success.

1.0 Guidance, Navigation, & Control

This document summarizes the NESC GN&C TDT's work to synthesize and document the current best practices for the design & development of robust and reliable GN&C systems for robotic and crewed (human-rated) spacecraft. These GN&C best practices for future science and exploration missions were derived from the lessons learned, both positive and negative, on earlier spaceflight projects, both robotic and crewed. An attempt has been made to capture preferred practices that reflect the key considerations, trades, and processes directly attributed to past mission success. In this section of the report, the GN&C interactions with other spacecraft systems will be highlighted and a high-level GN&C DDT&E process will be described. Subsequently, a discussion of GN&C robustness, reliability, and fault tolerance issues, as illustrated by the history of crewed and robotic GN&C missions, will be presented. Lastly, the specific engineering best practices that yield a robust and reliable GN&C subsystem are listed. Wherever possible, relevant linkages are established between the best practices and specific lessons learned from past space mission failures and mishaps.

The purpose of this section of the report is to provide useful guidance, in the form of best practices and other considerations and criteria, to the formulation, architecture, design, development and operation of GN&C systems for NASA's future human-rated spacecraft. It is sincerely hoped that engineers and managers can use this information as an experience-based checklist that will increase design consistency, increase efficiency of the overall DDT&E effort, and most importantly, increase confidence in the safety and reliability of the human-rated spacecraft's GN&C end product.

1.1 Introduction to GN&C Subsystem Engineering

The term *GN&C* covers a broad range of spacecraft engineering activities and specialties related to determining and controlling the dynamic state of a vehicle as necessary to meet mission objectives. A spacecraft's GN&C system is critical to executing space mission operational functions, such as orbital insertion; Sun acquisition; Earth acquisition; target acquisition; pointing and tracking; rendezvous; orbital/trajectory Delta-V propulsive maneuvers; entry, descent and landing attitude maneuvers; and velocity changes, as well as the articulation of

multiple platform appendages such as solar arrays and communications antennas. The functional definitions for GN&C that will be adopted for this discussion are the following:

The function of a spacecraft GN&C subsystem is to determine and to control the position, velocity, acceleration, attitude (i.e., orientation), and attitude rate of the spacecraft, with respect to prescribed coordinate reference frame(s), in a manner that satisfies requirements for all mission phases.

1. ***Guidance*** is the determination of a trajectory from a current position/velocity/attitude state to a desired position/velocity/attitude state, satisfying specified costs and constraints, such as fuel expenditure, safety, dynamic/thermal loading, and time criticality. Real-time guidance laws are embodied as time-critical algorithms implemented in the FSW, which runs on the spacecraft processor. In non-real-time applications, guidance law computations are executed in ground computers to determine the guidance commands, which are then uplinked to the spacecraft. In either case, these algorithms must provide safe, stable, efficient trajectories throughout different mission phases, spacecraft configurations, and operating modes.
2. ***Navigation*** is the determination of the current dynamic state of a moving platform in a specified coordinate frame. Navigation is implemented by using a specific sensor suite that provides data to the FSW navigation algorithms, either in a raw format or pre-processed by a navigational receiver. This sensor data are processed to determine the best estimated spacecraft position, velocity, acceleration, attitude, and attitude rate at a given time with respect to a selected reference frame.
3. ***Control*** is the determination of the commands to the spacecraft's force and torque actuators that regulate the vehicle's six degree-of-freedom (DoF) motion. The primary role of the spacecraft controls is to maintain vehicle stability at all times while driving the navigated state to the desired guidance state by issuing commands to the appropriate actuators. Automatic feedback control systems employ sensors to measure and compare the guidance-generated input commands with the output responses. Control system feedback compensation ensures stable motion for spacecraft attitude pointing/tracking operations for all mission phases, including large re-orientation maneuvers as well as orbit maintenance/trajectory correction propulsive maneuvers. Control involves algorithms encoded into spacecraft FSW, or embedded into the micro-controllers of servo-electronic mechanisms, as well as actuators for active control through mass movement (e.g., reaction wheels and control moment gyroscopes (CMGs)) or mass expulsion (e.g., engines, thrusters, and jets). Depending on the spacecraft design and mission phase, there may also be aerodynamic control surfaces, parachutes, and brakes used for controlling the vehicle.

1.2 Overview of GN&C Section

Best practices for future missions derive from lessons learned, both positive and negative, on earlier programs. The space system GN&C engineering best practices documented in this report reflect key considerations, trades, and processes directly attributed to past mission successes.

This section highlights the interactions of GN&C with other subsystems, providing the discussion for Best Practice #1 in Section 1.6.

Section 1.3 covers the high-level GN&C DDT&E process, emphasizing the subdivision of the overall DDT&E activity into distinct phases: Early Work and Late Work. The key steps in the GN&C DDT&E process are identified, as are typically encountered problems and issues.

Section 1.4 focuses on robustness, reliability, and fault tolerance issues illustrated by the history of crewed and robotic GN&C missions, highlighting lessons learned and linking the reader to the related best practices.

Section 1.6 is the heart of this GN&C discussion, and the reader's attention is directed there to view key GN&C-related findings of this study. This section presents specific engineering practices that yield a robust and reliable GN&C subsystem. A comprehensive list of 22 GN&C best practices, as identified by this NESC study, is provided. The many and varied sources used to uncover and gather this super-set of GN&C best practices will be described. These 22 best practices are divided into two major categories, consistent with the overall philosophy of this report: one category that applies to the Early Work phase of the overall DDT&E effort and another that applies to Late Work. The first set of best practices (1 through 15) applies principally to the early GN&C engineering activities associated with "Architecting the Right System," whereas the second set (16 through 22) applies to the later stages, focused on the end goal of **"**Building the System Right." Furthermore, readers will see that a standardized approach is employed to present each GN&C best practice. Each best practice is cited, then followed by a supporting technical discussion to describe, expand upon, and amplify its significance. Then, wherever possible, relevant linkages are provided to specific space mission and/or spacecraft lessons learned extracted from various NASA databases and other sources. These linkages are provided to showcase tangible real-world examples of mission failures and spacecraft mishaps that have occurred in the past as a direct result of not applying or adhering to the specific GN&C best practice cited. Lastly, a set of relevant questions is listed. These questions have a dual purpose. Primarily, they identify specific detailed areas for reviewers to probe as an aid in determining whether (and how well, and to what extent) the cited best practice is being adhered to by the GN&C development team being reviewed. Secondarily, the questions provide another means of exposing and highlighting the underlying nature and detailed aspects of the specific practice being cited.

1.3 GN&C Interactions with Other Subsystems

The GN&C subsystem is a mission-critical element in NASA's human-piloted and robotic spacecraft. A key point that repeatedly emerges from the review and evaluation of GN&C Lessons Learned over the years is the need to search out, identify/recognize, and acknowledge the strong interdisciplinary relationships that often exist between GN&C and other spacecraft subsystems. As Ryan stated in his 1985 report [ref. 1],[4] the design of high-performance and dynamically complex space systems can produce flight articles with a high sensitivity to parameter variations and reduced margins of stability and safety. More importantly, Ryan also stated, based upon his experiences during the Apollo, Skylab, and Shuttle Programs, *"In space systems, most dynamic problems do not occur in one isolated discipline, but are an interaction between several disciplines or subsystems."* So true.

[4] Please note that in Section 1 of this document, unless otherwise stated, the references called out are from Section 2.2, Original Report References.

GN&C subsystem engineering typically interacts with almost all of the other spacecraft subsystems. Figure 1.3-1 is an influence diagram depicting these multiple mission-critical interactions. An extremely important role of the GN&C SE is communication and coordination with other spacecraft subsystem leads. GN&C requires closing the loop around vehicle and human dynamics; therefore, it is of utmost importance to understand how faults in other subsystems will affect GN&C.

Figure 1.3-1. GN&C Subsystem Influence Diagram

GN&C functionality is composed of hardware and software components. In many modern spacecraft system architectures, these components are scattered across several subsystem elements. This introduces challenges unique to GN&C, since the GN&C function must levy requirements upon each of those subsystems and ensure appropriate elements work together to achieve GN&C functionality and performance.

Tables 1.3-1 and 1.3-2 indicate the GN&C subsystem's driving interactions, often in the form of derived requirements, with the other subsystems. Experience has shown that the path of ignoring, over-simplifying, or overlooking the critical need for compatible design interactions among the subsystems is a perilous one.

Table 1.3-1. Driving Interactions from GN&C to Other Subsystems

GN&C	– GN&C subsystem power consumption by mode or phase – Special GN&C component power regulation and conditioning required – Solar array drive pointing and tracking command signals	**Power**
	– Redundant jet orientations and/or gimbaled engine DoF and range required for control fault tolerance, force/torque constraints – Requirements for CFD modeling of liquid propellant slosh motions – Requirements for liquid propellant management (e.g., anti-slosh) devices	**Propulsion**
	– Minimum requirement for crew module lift over drag (L/D) ratio for entry flight path control – Aerodynamic parameters for launch abort scenario stability and control analyses	**Aerodynamics**
	– Special thermal range, gradient or stability required for GN&C sensors or actuators – GN&C power dissipation changes with equipment in use/modes creates different thermal loads & load variations due to changes in power profile	**Thermal**
	– Mass properties constraints – Constraints on flexible mode frequencies – Sensor size, placement, harnessing, and field of view (FOV) interference requirements – Sensor orientation, distribution, or FOV required for operation and fault tolerance (not just sensor orientation, but on-orbit orientation alignment stability)	**Structure**
	– Flight processor throughput/memory sizing, and fault tolerance – Time-critical interface concerns (real-time, deterministic) – Sensor readout and actuator command delays – Command/data interfaces – Downlink telemetry/status data timeliness, format, and bandwidth – Validation and confirmation of uplink commands	**Avionics**
	– Algorithms – Time-critical processing concerns – Fault tolerance – Units – Coordinate frames – Data formats – Fault detection/isolation of the sensor suites (processing/switching required on sensor suites) data monitoring needs (BIT, trending, algorithm, filter bounds)	**Software**
	– Mission phase functions: manual versus automatic capabilities – Mission phase: contingency plans, capabilities, limitations	**Crew**
	– GN&C telemetry parameters, data rates and scaling for nominal and contingency operations (dwell telemetry and diagnostics) – Establishment of valid GN&C telemetry limits for crew and ground displays, as well as establishment of valid thresholds for yellow caution and red alarm telemetry monitors	**Communications**
	– GN&C state information for safing reconfigurations	**Payload**
	– Backup of GN&C/crew – Restart/reinitiate capabilities and needs – GN&C failure modes/limitations and recovery paths – Indications of GN&C failure – Requirement to provide high-level mission plan/re-plan sequence – Primary position reference information	**Ground Control**

Table 1.3-2. Driving Interactions from Other Subsystems to GN&C

Power	– Available launch/early orbit battery power for despin and initial acquisition – Solar array pointing and tracking control interface – Redundancy of power sources – Power available: regulation, transients, high-low limits – Frequency and amplitude of disturbances from solar array drive(s)	**GN&C**
Propulsion	– Propulsive actuator interface functionality and performance: scaling, linear vs. pulse, operating constraints, response times – Number of thrusters, distribution, orientation, thrust inefficiency, thruster control authority, minimum impulse bits – Thrust Vector Control (TVC) gimbal DoFs, dynamics and range of motion, TVC gimbal friction – Plume impingement force/torque disturbances, de-stabilizing liquid propellant sloshing dynamics, energy dissipation – Propellant tanks, manifolding, valves, tank baffles and/or management devices (PMDs)	
Aerodynamics	– Analytic and wind tunnel predictions of L/D ratio for crew module entry flight path control – Atmospheric model density predictions	
Thermal	– Special attitude maneuvers and orientations required for thermal control and/or thermal safing (e.g., solar avoidance or solar intrusion constraints) – Temperature gradients (diurnal and mission variations) – Nominal and extreme temperatures (survival and operating)	
Structure	– Mass properties for stability, center of gravity location, and knowledge of location – Disturbance and vibration sources and isolation – Destabilizing flexible body or modal dynamics and controls-structures interactions	
Avionics	– Data bus architecture and on-board computer for real-time-critical GN&C processing – General-purpose computer configuration and fault detection, isolation, and recovery (FDIR) reporting – Data storage – Available time reference/time reference maintenance – Ground communications (up and down)	
Software	– FSW code and data for real-time-critical mode-dependent GN&C processing – GN&C mission support ground software, ground software to FSW interface – Mechanisms (performance that gets flagged) and indications of fault status/switching actions – Options to intervene in software routines by ground or crew – Access to intermediate calculations, algorithm inputs/outputs	
Crew	– Displays, monitors, alarms, and control input devices – Manual control requirements and capabilities – Manual abort requirements and override capabilities – Training and associated training simulators/facilities	
Communications	– Frequency and amplitude of disturbances from antenna positioning mechanism(s) – Antenna pointing and tracking control interface – Interference (glinting, masking and shading) of critical GN&C sensors and thrusters due to antenna motion	
Payload	– Image quality requirements (e.g., jitter and smear requirements, vibration susceptibility) – Agility requirements (e.g., large-angle slew requirements, re-pointing frequency requirements) – Frequency and amplitude of disturbances from payload scanning/steering/pointing mechanism(s) – Payload control signal interfaces for safe-mode and other possible functions – Fine guidance sensor error signals from payload to augment pointing	
Ground Control	– GN&C status/failure/loss of function indications – Intervention capabilities/ ops contingency modes – Command/confirmation structure and execution sequence and reporting – Precision of ground navigation info, regions where available/unavailable	

1.4 Overall High-Level Design Process/Drivers

The typical GN&C design and development process poses challenging and complex technical problems for an engineer. GN&C is a broad area that encompasses many areas of engineering, mathematics, and science, such as:

- Attitude, orbit, and trajectory analysis and mission design.
- Automatic feedback control system design and analysis (from single-input/single-output servo-mechanism loops to multivariable controllers with many interacting loops).
- Dynamics (spanning the range from simple single rigid body dynamics to complex multiple interconnected flexible bodies with energy dissipation).
- Kinematic analysis.
- Avionics and instrumentation.
- Navigation (including attitude) sensor hardware design, development, integration, and operation.
- Actuator hardware design, development, and integration operation.
- Sensor and actuator calibration.
- Modeling and simulation.
- Optimization techniques.
- Estimation filter design (e.g., Kalman filtering for attitude determination).
- Algorithm design and development.
- System integration and test.
- Flight operations.

The design and development process is typically led by a GN&C SE supported by a core team of mission trajectory/orbit designers, dynamists, control system analysts, attitude determination/estimation specialists, navigation engineers, sensor/actuator hardware engineers, and simulation/test bed development specialists. The primary responsibilities of the GN&C SE are to sufficiently coordinate with the stakeholder (which could be the Project Office or, in some cases, the actual end user/customer) to fully understand the mission-level GN&C design drivers and to clearly define flow-down to others, and document the comprehensive set of GN&C requirements.

The overall GN&C system DDT&E process flowchart is depicted in Figure 1.4-1. Later in this report, Figures 1.5-1 and 1.5-2 will lay out the GN&C-specific DDT&E process in a detailed format.

Figure 1.4-2 provides a broad aggregate list of potential threats to a successful GN&C system DDT&E process. It is highly unlikely that any single system development would fall victim to all, or even many, of the items depicted in the notional "GN&C Threat Cloud." An examination of the historical record does reveal, however, that several GN&C systems have been seriously victimized by one or more of the items called out in Figure 1.4-2, either during their design, development, test, or operational phases.

There are several points to be emphasized here: Spacecraft GN&C design and development mistakes are being repeated by projects. Lessons learned from past failures and mishaps are not being sufficiently infused into NASA's day-to-day GN&C engineering processes. It also appears that many previously established lessons learned must be relearned. The continued repetition of

the same GN&C mistakes poses a risk to mission success that is potentially avoidable. GN&C engineers would be well served to keep this list of "what can go wrong" pitfalls in mind as they perform their daily job functions. Design reviewers could also use the items called out in Figure 1.4-2 as a top-level checklist to prompt inquiries into areas that have historically been problematic for GN&C system development. More importantly, the set of GN&C engineering best practices identified in Section 1.6 will serve as a resource for GN&C engineers. If rigorously adhered to, these GN&C best practices can effectively protect against the threat items cited in Figure 1.4-2.

Lastly, before leaving this general discussion on the GN&C design and development process, it is imperative to touch upon the importance of conducting early architectural trade studies. The choice of architecture affects the way in which systems are designed, built, tested, and operated. In reference 30, Crawley and his co-authors describe/summarize, in an abstract manner, the role and influence of architecture in the process of creating complex systems. They argue for the importance of architecture as a determinant of system behavior. Architectures are not static, but evolve over time. Architectures have behaviors that no subsets of their constituent elements have. These higher-level architectural behaviors are the by-product of all their inter-element interactions. The fundamental aim of the architectural development process is therefore to obtain the desired behaviors (i.e., functional performance plus all associated "-ilities") while suppressing the undesired behaviors.

History, especially the Apollo Program, shows the value of performing early up-front "architectural design trade" work. Robustness and reliability must be "architected in" as part of the early steps of the GN&C systems engineering process. It is relatively easy to identify a superior GN&C architecture. It is one with the desirable attributes of allowing for growth in the mission set and possessing high measures of effectiveness, safety, reliability, affordability, and sustainability. Inferior architectures may be overly complex and are typically difficult to produce, test, operate, support, service, and upgrade. They are often prohibitively costly to adapt to evolving mission scenarios as the life-cycle extends beyond the anticipated timeframe of the spacecraft's service life. An inferior GN&C architecture can be brittle, with few robustness qualities.

The selected architecture will directly influence the physical complexity, functional behavior, and performance of the GN&C subsystem, along with the related properties of safety, ease of implementation, operational complexity, affordability, robustness, serviceability, adaptability, flexibility, and scalability. As will be described under Best Practice #1 (Section 1.6), architectures for most human-rated spacecraft GN&C subsystems are typically formulated via multiple closed-loop iterations between the architect team, system designers, and the stakeholder community. During the architectural development process, the mission requirements, operations concept, and architecture/system design are all traded off against each other and against some risk posture for the program. Coordinating and directing those iterative interactions and ensuring they occur early and converge soon enough to facilitate management decisions is an important GN&C SE responsibility.

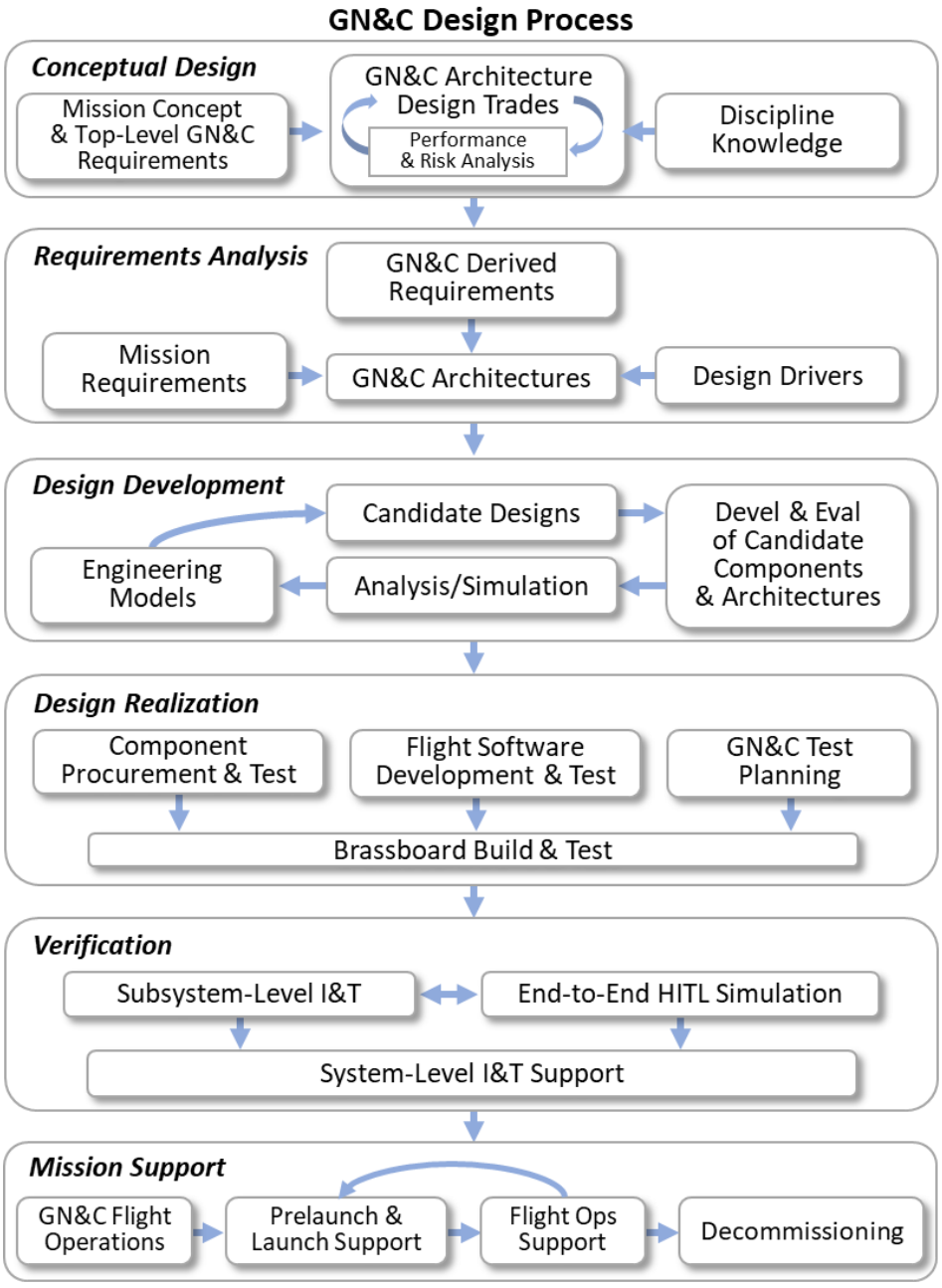


Figure 1.4-1. Overall GN&C DDT&E Process

Figure 1.4-2. The GN&C Threat Cloud

1.5 History with Links to Best Practices

This section provides a historical perspective on the topics of GN&C systems, safety, robustness, reliability, and fault tolerance. The history of select crewed and robotic missions is discussed to review relevant GN&C system DDT&E experiences, highlight the lessons learned, and link readers to the related best practices.

1.5.1 GN&C History for Crewed Spacecraft

The basic GN&C architecture and evidence for early-stage analysis and design will be discussed here for the last three crewed programs: Apollo, Shuttle, and the International Space Station (ISS). Discussions of the robustness, reliability, redundancy, and fault tolerance of the selected GN&C architectures for each of these programs are also included, along with the steps taken in the late development, integration, and test phases to achieve the design intentions.

The historical record shows clearly that U.S.-crewed space efforts all conducted thorough analysis and design trades early in their development. They performed GN&C architecture trades in the context of mission concepts and risk evaluation. The chosen architectures varied widely among programs, which is not surprising given their very different mission objectives and requirements.

Apollo

The goal of the Apollo Program was to place human exploration teams on the Moon and return them safely to Earth. A spacecraft consisting of three modules was launched on a trajectory to the Moon by a Saturn V launch vehicle. The Command Module, designed for atmospheric re-entry, was the home for the three-man crew during most of the trip. The Service Module provided maneuver propulsion, power, and expendable supplies, and was jettisoned before re-entry into the Earth's atmosphere. The Lunar Module (LM) was the vehicle that actually made the lunar descent. The module carried two crew members to the lunar surface while the other two modules remained in lunar orbit. It then returned to lunar orbit, rejoined with the Command Module, and was jettisoned after crew transfer.

A concise description of the primary GN&C system for the Lunar and Command Modules is provided in reference 2. In the report, one of many written in the early 1970s to document the design and development experiences of the Apollo Program, the Apollo primary guidance system is traced from the initial adaptation of the Polaris A-3 guidance system through its evolution from Block I to Block II configurations. A discussion of the design concepts used, as well as the test and qualification programs performed, is also included. The report documents the heritage and evolution of the Apollo navigation sensors and guidance computer. Among the technology mentioned is the use of Polaris gyroscopes and accelerometers, as well as computer design and real-time input/output interrupt concepts originally developed by Dr. Charles Stark Draper and his team at the Massachusetts Institute of Technology Instrumentation Laboratory (MIT-IL) for a Mars mission.

Early design trades and drivers were thoroughly analyzed before building and testing, as documented in the series of MIT-IL "E" reports. The performance requirements for the inertial subsystem, or indeed for the guidance and navigation system, were never clearly specified during the early program phases. The error analysis of the trajectories and early mission studies were performed by MIT, and a set of reasonable design specifications was formulated using the analysis results. From an inertial performance standpoint, the inertial measurement unit (IMU) error analysis revealed that moderate performance capability would suffice for crewed missions. The most critical parameter was identified as the gyroscope bias drift, which was the result of the long period between alignment and thrust termination. The analysis also indicated that rather large errors in acceleration sensitive gyroscope drifts could be easily tolerated, as well as moderately large-scale factor errors. A decision was made to conform to the more demanding Polaris A-3 missile inertial system performance requirements because of two factors: 1) the early Apollo test flights were to be uncrewed, thus not permitting the alignment, and 2) the tighter performance requirement would be indicative of and conducive to higher reliability. Another factor in the decision to adopt the tighter IMU performance specifications was that at this early point in the Apollo Program, the flight duration and flight path trajectories of the uncrewed test missions had not yet been established. By deciding early to go with the higher-performance IMU, program managers were able to compensate for this uncertainty in the definition of future

missions and also to avoid any downstream IMU retrofit cost and schedule impacts. Indeed, as it turned out, because of the variety of mission profiles flown, a different inertial system error component was predominant for each of the uncrewed Apollo test flights [ref. 2].

The success of the Apollo Program is considered evidence that this early design work constitutes a best practice. Design drivers and trades included:

- Navigation instrument selection.
- Three-gimbal versus four-gimbal IMU platform trades.
- Mission phases and duration.
- Program schedule and resources.

The Apollo-era reports reviewed as part of this NESC study consistently stressed the importance of defining the design environment and early and late testing to evaluate the design and workmanship against this environment. In one such report [ref. 3], Dr. George M. Low listed, *"Three of the basic ingredients of the success of Apollo: spacecraft hardware that is most reliable, flight missions that are extremely well planned and executed, and flight crews that are superbly trained and skilled."* The report is a series of eight articles reprinted by NASA under the collective title of "What Made Apollo a Success," used with permission, from the March 1970 issue of Astronautics & Aeronautics, a publication of the American Institute of Aeronautics and Astronautics (AIAA).

In his own 1969 AIAA paper [ref. 4], simply titled "Apollo Spacecraft," George Low also attributed the overall Apollo success to reliable hardware, thoroughly planned and executed flight operations, and skilled, superbly trained crews. Major factors contributing to spacecraft reliability are simplicity and redundancy in design, an emphasis on tests, a disciplined system of change control, and closeout of all discrepancies. In the Apollo design, the elimination of complex interfaces between major hardware elements was also an important consideration. The use of humans in flying and operating the spacecraft evolved during the course of the program, with a tendency to place more reliance on automatic systems. However, the capability for monitoring and manual takeover was always maintained. The spacecraft test effort was increased during the 18 months preceding the first crewed flight, with emphasis on environmental acceptance testing. This test method screened out a large number of faulty components prior to installation [ref. 4].

Clearly, the success of the Apollo missions was attributable in large part to the program's philosophy of "Testing to Ensure Mission Success" [ref. 3, chapter 3, by Scott H. Simpkinson]. The concept of allowing ***no*** unexplained test failures was the foundation of a discipline that enabled success to be achieved in the complex national goal called Apollo.

The different types of testing employed revealed numerous design and development problems. Time and effort were expended early on to formally define design environments for Apollo: acceleration, vibration, shock, temperature, humidity, pure oxygen atmosphere, electrical input power, pressure, etc. Subsequently, two major Apollo test phases were executed:

- Design evaluation testing: This testing was performed early in the design phase, using mockups, prototypes, and first-article development hardware to ensure that the equipment as designed did indeed have the integrity and capability to meet and exceed performance requirements and determine and define margins and design limitations in excess of requirements. The design of each element was rigorously examined with regard to thermal

evaluation, mechanical integrity, marginal voltages, vacuum, functional and operating characteristics, stability, alignment, system integration, and interface requirements. Other peculiar characteristics or environments to which a particular element was sensitive, such as humidity, salt, contaminants, and electromagnetic interference, were also examined.
- Formal qualification testing: The goal of this test program was to ensure performance under mission environmental conditions.

An example of a major problem area for GN&C revealed by testing was the contamination of the Apollo IMU gyroscopes during production. Testing also revealed gyroscope wheel bearing failures due to extended operational hours.

More detailed descriptions of the GN&C system, its designs, and the design approach can be found in the MIT-IL R-700 Final Report series, Volumes I-V, which documents the role of MIT in Project Apollo [ref. 64]. In particular, the evolution of the Apollo inertial subsystem design is described in Volume IV of that report, which discusses the following topics:

- Historical background of the Apollo GN&C
- Gimbal system arrangement
- Design characteristics
- Component selection
- Gyroscopes, accelerometers, component configuration control, component data management
- IMU design
- IMU angle resolvers, temperature control
- System design consideration

The sections referenced above discuss the process the team went through to translate mission needs into designs that would work under the given weight and power constraints. Similar conceptual design considerations and trades are documented for the optical subsystem and the guidance computer (Section 1 in both Volumes II and III). The historical background in Volume IV points out that the Apollo GN&C work built upon a 1957-1959 MIT-IL study on a recoverable interplanetary probe, which identified the required onboard sensors for spaceflight. The MIT-IL team also leveraged the Polaris missile GN&C system development results for the Apollo GN&C [refs. 5–7].

The Apollo GN&C system was a single-string mechanization with no redundant features. Mission success required a fully functioning system. Several aspects of the program's execution (the "Late Work" phases of the DDT&E process) that produced the robustly performing system were an emphasis on component reliability, extensive testing, built-in fault responses, and early and thorough crew participation and training.

The robustness of the system resulted from testing and qualifying to a conservative, formally defined design environment. To achieve component reliability, rigid quality control processes were developed and applied on all parts used, with special NASA fabrication lines using NASA-certified trained assemblers. Inspections of the build lines at the industrial contractors were continuously performed. Special reliability screening methods were put in place for the inertial components (e.g., gyroscopes and accelerometers). In one instance for gyroscopes, approximately 230 in a 270-lot build were rejected on the basis of a "failure prediction screening test." At the electronic device level, all devices were tested. If a sample in a run proved

defective, the entire lot was quarantined. Failed devices went through detailed teardown failure analysis to preclude defect migration problems.

Extensive component-level testing, stress testing, and integrated GN&C system testing was performed. A flight readiness certification was made on all systems. Integrated system-level tests were conducted at MIT-IL and JSC.

The Apollo computer's ability to detect faults using built-in test circuits was provided, since it was known that digital equipment was sensitive to transient disturbances and a method of recovery from transient faults was desirable. The outputs of these fault detection, isolation, and recovery (FDIR) circuits generated a computer restart, i.e., transfer of control to a fixed program address. In addition, an indicator display was turned on. If the fault was transient in nature, the restart would succeed and depressing the error reset key could clear the restart display. If the fault was a hard failure, the restart display would persist and a switch to a backup operating mode was indicated.

Apollo astronaut participation in the development cycle was typical, intensive, and necessary. It resulted in several design changes that enhanced manual operation. In addition, this training proved invaluable in handling contingency problems that arose during flight missions.

In reference 8, Hoag provides an excellent, succinctly readable history of the on-board Apollo GN&C system development written from the point of view of someone who personally experienced that process.

In closing this section, it is fitting to repeat the words of Dr. Charles Stark Draper, from the foreword of the MIT-IL R-700 final report [ref. 64]:

> *Man's rush into spaceflight during the 1960s demanded fertile imagination, bold pragmatism, and creative extensions of existing technologies in a myriad of fields, The achievements in guidance and control for space navigation, however, are second to none for their critical importance in the success of this nation's manned lunar-landing program, for while powerful space vehicles and rockets provide the environment and thrust necessary for space flight, they are intrinsically incapable of controlling or guiding themselves on a mission as complicated and sophisticated as Apollo. The great achievement of this Laboratory was to supply the design for the primary hardware and software necessary to solve the Apollo guidance, navigation and control problem. It is to the credit of the entire team that this hardware and software have performed so dependably throughout the Apollo program.*

Skylab Orbital Workshop

Skylab was the first U.S. orbital workshop, or "space station." Skylab was launched on May 14, 1973, on a Saturn V booster. The Saturn V's first two stages put the empty but modified S-IVB third stage, the so-called "wet workshop," into orbit. The S-IVB contained the workshop, which included a solar telescope mount and crew living and working quarters. Mission plans had nominally called for the first crew to fly the following day to Skylab on an Apollo-type Command Service Module (CSM) vehicle launched by a Saturn-IB booster. However, 63 seconds after liftoff, the meteoroid shield, which had the dual purpose of thermally shading the workshop, inadvertently deployed. It was torn from the vehicle by atmospheric drag forces. This

anomaly triggered a two-week period in which Skylab was challenged by problems that had to be overcome before the vehicle would be safe and habitable for the three crewed periods of its planned eight-month mission.

When the meteoroid shield ripped loose, it disturbed the mounting of workshop solar array wing number two and caused it to partially deploy. The exhaust plume of the second-stage retro-rockets impacted the partially deployed solar array, literally blowing it off the Skylab vehicle. In addition, debris from the meteoroid shield overlapped solar array wing number one such that when the programmed deployment signal occurred, the wing was held in a slightly opened position, unable to supply sufficient electrical power for the entire workshop. Finally, the gyroscopes were drifting because of their high off-nominal operating temperatures.

These failures caused concern that the interior of the space station would overheat and destroy equipment. The damage was so serious that mission controllers felt Skylab would be functional for only a short period before failing. However, by using the computer system that controlled the workshop's attitude, the ground controllers were able to manage the vehicle's attitude and keep Skylab alive. Orientation was kept at angles to the Sun, such that tolerable workshop temperatures could be maintained while simultaneously providing enough illumination on the remaining solar panels to generate sufficient electrical power. At times, these thermal management and power generation requirements were in opposition and operational priorities and trades were performed to balance thermal-power attitude conflicts. The condition that maintained the most favorable balance between Skylab temperatures and its power generation capability occurred at approximately 50° nose-up. This had to be done for a period of about two weeks while engineers prepared materials for the first Skylab crew to take into orbit to repair the orbital workshop.

Three separate crews were launched to Skylab on Apollo CSM vehicles by Saturn IB launch vehicles on May 25, July 28, and November 16, 1973. The first Skylab crew spent many extravehicular activity (EVA) hours to deploy a parasol-type sunshield through Skylab's solar scientific airlock and to later release solar array wing number one. The repairs performed by the first crew made the remainder of the Skylab mission possible.

The attitude pointing and control system (APCS) for Skylab evolved from an analog controller into a fully digital processing system. Features included a software-determined attitude reference to provide general maneuvering ability, an on-orbit re-programming capability, the use of large CMGs for attitude control, and the use of vehicle maneuvers to desaturate accumulated CMG momentum. The objectives and requirements for Skylab were challenging, with the most stringent requirements imposed on the Skylab APCS by the science observations of solar, galactic, and Earth Resources phenomena. The science instruments requiring the extreme arc-second levels of pointing accuracy and stability were mounted on the Apollo Telescope Mount (ATM) spar, which could move with respect to the rest of the Skylab vehicle [ref. 62]. Skylab was unusual in this regard, as historically no crewed spacecraft had ever been used as a platform for precision science instrument pointing applications.

As mentioned, Skylab was the first large NASA human-rated space vehicle to be controlled by relatively large, double-gimbaled CMGs. Each CMG had a large-momentum wheel spinning at a constant speed of about 9,000 rpm, and control torques were generated by steering the direction of the wheel's spin vector with respect to the vehicle by commanding the CMG gimbals. The

CMGs could generate sufficient control torque for the large maneuvers needed for thermal control in the first week of Skylab's mission before solar shield deployment. They also could generate control torques for the smooth, moderately high, angular-rate attitude maneuvers required for Earth resources remote sensing (i.e., landmark tracking) passes. In addition, as mentioned in reference 61, the Skylab CMGs were used successfully during the mission to:

- Stabilize the vehicle against transients, such as crew motion disturbances.
- Store the momentum accumulated due to gravity gradient and venting disturbance torques.
- Reorient the vehicle with respect to the gravity field during the night portion of the orbit to reduce the stored CMG momentum.

A cold gas thruster system was included in the Skylab design to augment the CMG system when required. The cold gas thrusters could also be used to unload accumulated CMG momentum when necessary.

The third and last Skylab crew departed the vehicle on February 9, 1974. Following this final crewed mission phase, ground controllers performed a series of engineering tests of certain Skylab systems. These were tests that ground personnel were reluctant to do while the crew was aboard the vehicle. Results from these tests helped determine causes of failures during the mission and obtain data on long-term degradation of space systems. Upon completion of the tests, Skylab was positioned into a stable attitude and systems were shut down.

For much of Skylab's operating life, the flight computer system automatically managed vehicle operation. The entire system functioned without error or failure for more than 600 days of operation, even after a 4-year and 30-day interruption. It is significant as the first spaceborne computer system to have redundancy management (RM) software. The software development for the system followed strict engineering principles, producing a fully verified and reliable real-time program.

It was expected that Skylab would remain in orbit for 8 to 10 years. By that time, the new Space Shuttle was anticipated and mission planners envisioned using the Shuttle to boost Skylab into a higher orbit with lower atmospheric drag. However, unexpected solar activity in the mid-1970s resulted in an increase in atmospheric density, so Skylab's orbit decayed at a much faster rate than projected. In the fall of 1977, it was determined that Skylab was no longer in a stable attitude as a result of greater than predicted solar activity. On July 11, 1979, Skylab re-entered Earth's atmosphere. Although the spacecraft was destroyed, a significant number of debris objects survived the reentry heating and loads environment and impacted the Earth's surface. The Skylab debris dispersion area stretched across a narrow band from the Southeastern Indian Ocean across a sparsely populated section of Western Australia.

Looking back on the Skylab mission, several GN&C-related lessons were learned:

1) Skylab CMG Lubrication: Two of the Skylab CMGs experienced bearing anomalies (i.e., temperature increases), and one (CMG #1) failed on Day 194 of the mission. Analysis indicates that poor lubrication caused bearing failure. The CMGs were designed with an automatic lubrication metering system that was chosen to minimize the need for active control, maximize bearing life, and prevent contamination by containing all oil. Life tests conducted on the ground far exceeded the required life. In retrospect, it appears as if the forces on the oil in zero gravity caused it to seek different locations than in 1-g, where full lubrication was possible. The specific

lesson learned was that, if at all possible, positive lubrication methods should be included in the design of long-life rotating machinery like CMGs. Since fluid flow in zero-g is application-sensitive and not always fully understood, it is prudent to design a system with positive control [ref. 60].

2) GN&C Design Versatility and Flight Computer Flexibility: The digital control system, with its ground reprogrammable flight computer, proved invaluable during contingency operations. The implementation of the challenging thermal-power attitude profiles flown prior to installation of the sunshade and deployment of the jammed solar wing were possible because of the APCS design versatility and the operational flexibility afforded by the Skylab digital flight computer. Specifically, the following Skylab FSW code and data modifications were developed and used during the mission to adapt to changing mission circumstances and operational situations:

- Compensation for excessive gyroscope drift.
- Compensation for variable gyroscope scale factors resulting from different gyroscope temperatures.
- Accommodation of an additional star for better roll update information.
- Development of a program, loadable from the ground, that would have allowed vehicle control by derived rates if the rate gyroscopes had failed.
- Mass property updates in the computer, allowing more accurate momentum management.
- Provision in the software for improving experiment data accuracy if necessary.
- Improvement of attitude maneuver command granularity to facilitate viewing of the comet Kohoutek.

In summary, Skylab clearly proved that a redundant general-purpose digital flight computer, reprogrammable from the ground and backed up by an extremely versatile group of support personnel using a variety of simulations, made it possible to meet every contingency situation that arose during the mission [ref. 61].

3) APCS Verification: Skylab was probably the first large space vehicle where the primary means of attitude control system performance verification was solely based on computer simulation supported by limited hardware testing. This was a departure from past programs, where hardware testing was the major system verification technique. The software verification approach used in Skylab was dictated by the difficulty of testing a vehicle of such size and the fact that arc-second pointing performance measurement is not independent of test equipment errors. This approach yielded satisfactory system verification in a cost-effective manner. This approach will be even more applicable to future missions where performance requirements transcend those of Skylab for vehicles of similar or possibly larger size [ref. 61].

4) Structural Bending Mode Uncertainty: Flight data indicated that structural bending modes differed significantly in some respects from pre-flight analytical predictions. However, the control system design had sufficient margin to meet both pointing and stability requirements. The lesson learned is obvious: Realistic tolerances should be provided in the design when complete pre-flight verification is not possible [ref. 61].

5) Skylab Re-Entry: The lesson learned from Skylab's re-entry is that mission architects must plan ahead for the safe post-mission disposal, decommissioning, and/or de-orbiting of massive space platforms in low Earth orbits (LEO). A re-entry debris analysis should be performed to

assess the total risk level to people and property for both random re-entry and controlled re-entry de-orbit scenarios.

Space Shuttle

Born in 1968 at the height of the Apollo Program, the Space Shuttle was designed to fulfill two basic roles in NASA post-Apollo crewed flight objectives. The first program goal was to provide an efficient, re-usable method of carrying astronauts to and from a permanently crewed space station. In addition, NASA believed that Space Shuttles could serve as multi-purpose satellite delivery vehicles with the potential to completely replace Atlas-Centaur, Delta, and Titan rockets.

The Space Shuttle Avionics Handbook monograph [ref. 9, Section 3] details the navigation system design evolution—providing a record of Shuttle early work and design drivers. Section 4 of the same monograph discusses each of the GN&C functions: hardware required, use of the data processing complex, crew involvement, and RM features provided. RM features cover the fact that Shuttle carries duplicates of many sensors and actuators, and the monograph details the FDIR logic and contingency operation for the sensors or their functions. The following discussion contains extracts from the monograph.

Prior to the Space Shuttle, aerospace systems were made up of an essentially independent collection of subsystems, organized along disciplinary lines such as flight control, guidance and navigation, communications, and instrumentation. Each subsystem typically had dedicated controls, displays, and command and signal paths. The Space Shuttle avionics system not only integrated the computational requirements of all subsystems in a central computer complex, it also introduced the concept of multifunction controls, displays, and command/data paths.

The overall system design was driven by mission requirements and vehicle constraints never before encountered in a space program. Significant among these were the following requirements:

- Multiple reuses over a 20-year period. The economic and safety-related impacts of aborting after one failure required that the system have a two-fault-tolerant fail operational/failsafe configuration.
- Comparison of data or performance from independent systems or components operating in parallel as the primary means of detecting and isolating failures and assessing system operational status.
- Four parallel baselined strings to detect the second failure in a system.
- Excluding the use of a built-in test wherever possible as a less reliable fault isolation technique.
- An unpowered landing on a runway. The stringent performance required prohibited the use of degraded backup systems.
- Autonomy. Large quantities of instrumentation data, transmitted to the ground in previous programs for spacecraft functional assessment and subsystem management, had to be processed onboard and made available to the crew in usable forms.

The Space Shuttle vehicle that evolved was an unstable airframe requiring sufficient control authority to cause structural failure if an erroneously applied hardover control actuator command was allowed to remain in effect for as little as 10 to 400 milliseconds. Full-time stability

augmentation was baselined, direct control modes were excluded, and digital autopilots were designated to accommodate the wide spectrum of control. Manual intervention or switching of active/standby strings proved inadequate to overcome the effects of erroneous hardover commands; therefore, a system approach was baselined in which hardovers were prevented through the use of multiple, parallel-operating, synchronized processors, and command paths to drive force-summing control actuators.

The Shuttle GN&C system was designed to continue functioning despite some levels of component failure. The concept of a reusable orbiter significantly increased the operating time of the components, which were retested and recalibrated in situ before flight unless a failure or problem was reported.

Sophisticated guidance and navigation schemes and algorithms had been developed and used in the Apollo Program; therefore, the technology base appeared adequate for the Space Shuttle in these disciplines. Although a new guidance and navigation challenge was posed by the entry through landing phases, no state-of-the-art advances were deemed necessary. However, the early work for the design now included analysis of expected component reliability, expected fault and failure modes, and identification and elimination of common mode (single-point) failures as well as common cause failures. The architecture design included not just contingency planning, but also now RM. The integration of the computational requirements of all subsystems in a central computer complex and the concept of multifunction controls, displays, and command/data paths expanded the analysis work to include greater assessment of GN&C sensitivity and robustness to potential faults or failures in other subsystems.

The Space Shuttle Program did not rely upon the extreme process controls or stringent screening procedures that achieved reliability during the Apollo procurement. Consequently, problems of contamination during fabrication and failure due to extended operational hours were found with the Space Shuttle gyroscopes. At least six IMU failures were detected during flights, and several problems detected during preflight/prelaunch testing. However, due to the redundancy and RM system, there was no loss of IMU function during flights.

ISS

The objectives of the ISS Program are to develop a world-class, international orbiting laboratory for conducting high-value scientific research for the benefit of humans on Earth; provide access to the microgravity environment; develop the ability to live and work in space for extended periods; and provide a research test bed for developing advanced technology for human and robotic exploration of space. The purposes of the ISS GN&C system are to control the station's motion to be suitable for the intended uses of the facility and provide pointing and support information for appendages (e.g., solar panels, communication antennas). The ISS achieves robust, reliable GN&C through both functional and hardware redundancy.

The ISS GN&C system is made up of two components, one contributed by the U.S. and the other provided by the Russian Space Agency (RSA). The U.S. GN&C system consists of software installed on the U.S. GN&C multiplexers/demultiplexers (MDMs) and orbital replacement units. Note that the MDMs on the ISS are a combination of hardware and a computer processor. Onboard FSW estimates position and velocity by using one of three functionally redundant systems: the global positioning system (GPS) receivers and processors, Russian motion control system (MCS) data from the Global Navigation Satellite System (GLONASS), or ground

uplinks. The Russian Orbital Segment (ROS) MCS exchanges data with the U.S. GN&C MDMs, allowing for comparison and fault tolerance. Reboost is performed every 3 months to offset the effects of aerodynamic drag and raise the ISS's altitude. The primary method uses the Russian Progress main engine with fuel from Progress propellant tanks. An alternate method uses Progress rendezvous and docking thrusters with fuel transferred from the Zvezda or Zarya module. A third method uses the Zvezda main engines, but this is avoided as much as possible since those engines have a limited burn lifetime and cannot be serviced or replaced on-orbit.

The orientation of the core body is measured by interferometry of GPS signals in the U.S. GN&C system. The angular velocity of the core body relative to an inertial reference frame is measured with two rate gyroscope assemblies consisting of three ring laser gyroscopes (RLGs) each. The Russian MCS provides an alternate source of measurements for attitude determination, and data are continuously exchanged with U.S. GN&C MDMs. Russian sensors include star trackers, Sun sensors, Earth horizon sensors, magnetometers, rate gyroscopes, and GLONASS information. The sensors in ROS MCS include multiple layers of redundancy. The attitude of the core body is controllable by the Russian propulsion system or the U.S. attitude control system, which consists of two U.S. GN&C MDMs and four CMGs. The CMGs are relatively massive (about 300 kg each), with two-DoF gimbaled rotating flywheels. The CMG momentum manager algorithm is designed to keep the CMGs from saturating by maintaining the core body at a torque equilibrium attitude, an orientation in which the angular acceleration of the core body in inertial space vanishes: i.e., the resultant of gravity gradient torque, aerodynamic drag torque, gyroscopic torque, and other torques is zero. Russian reaction control system thrusters are used to desaturate the CMGs, hold attitude during reboost, and perform attitude maneuvers greater than 15° in magnitude [ref. 10].

Guidance is generally performed by the Russian MCS, although the U.S. GN&C system does provide a limited amount of guidance planning support. In addition, the Flight Dynamics Planning and Analysis tool is used by ground controllers and planners to provide high-fidelity trajectory, attitude, propellant consumption, and communications coverage analysis

Having both U.S. GN&C and ROS MCS systems onboard makes for many operational challenges. In response, control of the systems has been managed through the use of GN&C software modes. These modes provide flexible management of station operations and dictate which system is in charge of providing attitude control. This is critical to station operations, since only one GN&C system can safely control the vehicle at a given time [ref. 11, Section 7].

A discussion of several problems that occurred on the ISS in the spring of 2006 serves to positively emphasize the range of diverse redundancy and contingency plans available. The problems began on April 19, 2006, when the Russian Zvezda service module's main engines failed during a test. The failure may have been due to a sunshade cover that was not completely open, according to an ISS status report. It was the first engine test since 2000, when Zvezda first docked to ISS, then in its earliest stages of construction. The service module main engines were not planned to be used often because they cannot be replaced, unlike the Progress re-supply spacecraft, which periodically rendezvous and dock to deliver cargo to the station.

Subsequently, on May 4, 2006, the Progress ship docked to the station fired its engines for 6.5 minutes to boost orbit by 2.7 km. But after the thruster firing, the ISS crew received an error message saying the station software was not properly communicating with the Progress

hardware. Progress thruster firings controlled from within the ISS were ruled out until mission managers were able to successfully identify the problem and resolve the issue. One backup option was to have Russian ground controllers manually uplink in real-time the necessary commands to the thrusters to fire remotely. However, those commands can be uplinked only when the ISS is in contact with Russian ground stations; it is out of range for 6 of its 16 orbits every day. Another option to boost the ISS orbital altitude was to use the Russian Zvezda service module thrusters, distinct from its now-problematic main engines.

The Global Positioning System Receiver (GPSR) on the ISS was activated in April 2002. Since that time, numerous GPSR software anomalies have appeared and been resolved, in part, by extensive operator intervention (i.e., power cycling of the GPSR). Eventually, enough anomalies surfaced that the software in the GPS unit was rewritten and the GPSR units were upgraded. Reference 12 discusses the technical aspects of these ISS GPSR problems. The underlying causes that led to the delivery of a product that has had numerous problems are also covered there. These underlying causes include inappropriate use of legacy software (e.g., as occurred in the maiden flight of Ariane 5), changing requirements, inadequate software processes, unrealistic schedules, incorrect contract type, and unclear ownership responsibilities [ref. 12].

Similarly, reference 13 is a collection of writings concerning the application of GPS technology to the ISS, the Space Shuttle, and the X-38 vehicles. It provides an overview of how GPS technology was applied to each vehicle, including the rationale for the integration architecture, and the rationale governing the use (or non-use) of GPS data during flight. The Shuttle, ISS, and X-38 GPS projects encountered unanticipated technical, schedule and budget problems. In retrospect, the GPS technology proved to be more difficult to apply than was anticipated in the early 1990s. As a result of overcoming the problems, the Shuttle and ISS Programs eventually obtained and flew GPS receivers certified for operational use. Several lessons were learned during the requirements definition, integration, testing, certification, and operational phases of these GPS technology infusion projects. The author states that perhaps the most important lesson concerned the perceived maturity of GPS technology for space applications: Over-optimism about the ease of application of GPS to spacecraft-influenced budgets, scheduling and project planning led to several technical and project management problems [ref. 13].

History of Crewed Spacecraft Rendezvous and Docking

The capability to perform safe, routine, and reliable space vehicle rendezvous has been a basic operational building block of both the U.S. and the Russian human spaceflight programs since the mid-1960s.

The U.S. Apollo lunar landing missions were predicated upon the ability to perform lunar rendezvous between the CSM and the LM Ascent Stage. As described here, one of the primary objectives of the U.S. Gemini Program was to develop, demonstrate, and validate the technologies and operational methodologies necessary for a crewed spacecraft to execute space rendezvous and docking operations. The U.S. Space Shuttle Orbiter routinely performed LEO rendezvous maneuvers with the ISS and successfully rendezvoused with the Hubble Space Telescope multiple times to repair/service this national space science asset. The Shuttle Orbiter has also rendezvoused with the Russian Mir space station, as have many Russian crewed Soyuz spacecraft and robotic Progress re-supply cargo spacecraft. Russian Soyuz and Progress vehicles routinely rendezvous and dock with the ISS. The robotic European Space Agency (ESA) ATV,

Japanese HTV, and U.S. Cygnus re-supply spacecraft have conducted successful rendezvous and docking/berthing operations with the ISS as "visiting vehicles." The NASA Commercial Crew Program (CCP) SpaceX Dragon-2 spacecraft has successfully demonstrated the capability to rendezvous and dock with the ISS.

Similar to Apollo, in the near future NASA will require capabilities for lunar orbit rendezvous and docking to support plans for a U.S. human lunar landing in the 2015-2020 time frame. Given the payload lift constraints of current and projected launch vehicles, many future NASA mission architectures for Exploration will require the capability to perform space rendezvous, capture, and in-space assembly. In particular, an Autonomous Rendezvous and Docking (AR&D) capability will be critically required to make such operations routine, reliable, safe, and affordable. Multiple efforts are being pursued within NASA and by industry to develop and validate the technologies needed to implement an AR&D functionality. These AR&D-enabling technologies include GN&C algorithms, autonomous mission management, sensor technology, mechanisms, and robotic assembly techniques. These are at varying stages of technology readiness, but many are in a quite mature state. As pointed out by Zimpfer in reference 14, the key challenge in the development of any system to perform a rendezvous, capture, and assembly is the integrated system-level design, analysis, and validation. Many of the modeling tools, analysis techniques, and test approaches have also been developed to meet this challenge**.** In reference 15, Polites provides an excellent review of the technologies needed for automated rendezvous. Clearly, there is a critical need to sustain, advance, and improve the safety, efficiency, performance, and reliability of technologies, systems, and operational techniques for space vehicle rendezvous and docking.

The terminal, close-in phases of rendezvous and docking operations, as practiced to date in the U.S. human spaceflight Gemini, Apollo, and Shuttle programs, have typically been performed using a purely manual (or in some cases, semi-automatic) crew-in-the-loop technique. This crew-in-the-loop U.S. manual rendezvous method contrasts sharply with the automated approach to rendezvous and docking operations typically conducted within the Russian space program. Polites also provides a concise comparative history of U.S. and Russian space program approaches for and experiences with space rendezvous [ref. 15, Section 2].

Other important factors for space rendezvous are whether the target vehicle is cooperative (i.e., stabilized) or uncooperative (i.e., tumbling) and if the target vehicle has active targets (e.g., light emitting diodes) or passive targets (e.g., reflectors) for a chase vehicle terminal guidance sensor to track, or if the chase vehicle must use vision sensors and image recognition techniques for terminal guidance.

Space rendezvous and docking is, however, an inherently difficult and potentially dangerous operation. It requires detailed knowledge of the rendezvous target. The orbital, or in some cases trajectory, characteristics of the target need to be known to a suitable tolerance, as defined by analysis, and techniques for computationally propagating the target's state vector during the rendezvous engagement must be performed with appropriate accuracy. Characteristic features of the target must be defined to select and refine appropriate rendezvous sensor technologies. Typically, these characteristics include parameters like the target's radar cross-section, infrared signature, and sunlight glint/reflection properties. In the terminal phases of a rendezvous engagement, precise knowledge of the target's attitude motion and stability is required as well as an in-depth understanding of relative close-in dynamic interaction. For example, thruster

pluming of the target vehicle could dynamically disturb the target, complicating the physical docking process or damaging delicate structures (e.g., solar photovoltaic arrays or radiators) and/or contaminating exposed surfaces (e.g., payload optical surfaces).

Rendezvous and docking, as well as undocking and departure, are inherently dangerous operations because there is, by the very nature of the engagement, a risk of collision between the chaser and the target. The close-in phases of a space rendezvous and docking process typically involve the relative 6-DoF sensing and control of two vehicles with acceleration, braking, steering, and orientation controlled by thrusters or perhaps a combination of thrusters and reaction wheels. One simple technique to minimize risk is to employ a rendezvous scenario that includes a loitering mode in a nearby orbit with respect to the target that enables opportunities for system readiness checkout prior to initiating proximity operations.

Another technique is for the chase vehicle to enter a safety ellipse mode and slowly approach the target vehicle from the V-bar direction along the orbit velocity vector and from either behind or in front of the target vehicle. In this case, the total relative velocity of the chase vehicle is never in the direction of the target vehicle, avoiding the possibility of a collision. Typically, the preferred technique for Shuttle Orbiter rendezvous is the V-bar approach because, among other factors, the constant Earth horizon orientation is a good piloting reference and terminal rates can be easily and immediately nulled with subsequent efficient stationkeeping should some Orbiter, payload, or target vehicle anomaly occur [ref. 58]. Still another technique is to approach the target vehicle from the R-bar direction along the orbit radius vector and underneath the target vehicle. The R-bar approach is sensitive to targeting accuracy (i.e., large targeting errors could lead to a collision) and may require near-continuous thruster firings due to orbital period mismatch. Therefore, it is less fuel-efficient than the V-bar approach. However, the R-bar approach has the advantages of being passively safe and providing a consistent viewing angle to the target. In the event of an abort, for example, in the case of a single-point failure in the chaser's rendezvous sensor, thruster firings by the chaser will be terminated and the rendezvous operation can be passively aborted. In a passive abort scenario, the chaser vehicle will naturally move away downward and ahead of the target vehicle due to the relative orbital dynamics between the target and the chase vehicles.

A “hard” docking of chase vehicle to target vehicle occurs at some non-zero relative velocity to connect the two vehicles. The risk here is that if the hard docking is unsuccessful, then both vehicles are set into motion, which in itself could cause them to collide. In addition, the target vehicle may not have the means to restabilize itself, which could rule out a second docking attempt. One alternative is a “soft” capture, which is like a zero-velocity dock. Here, the two vehicles have docking mechanisms that allow a soft capture or partial connection at essentially zero relative velocity. Once a soft capture is achieved, the docking mechanisms are activated to mechanically complete the connection process. Another alternative to a hard docking is to “berth” one vehicle to another. Here, the chase vehicle gets close enough to the target vehicle so a robotic arm on one can grab the other and bring them together. This approach requires a robotic arm capable of maneuvering the chase vehicle, as well as the support of the ground operations team and/or the crew in one of the vehicles to perform the berthing operation.

As a case in point, the Shuttle Orbiter performs a hard docking with the ISS using the Androgynous Peripheral Attach System (APAS). The APAS is the spacecraft docking mechanism employed on all ISS docking ports. The APAS device was designed and built by the

Moscow-based RSC Energia organization, and its design origins date back to the Apollo-Soyuz Test Project (ASTP) of 1975. It is used to dock the Shuttle Orbiter vehicle and to connect the Zarya functional cargo block to the pressurized mating adapter on the ISS. Russian spacecraft use the same APAS device to mate with the ISS at the other docking ports on the Russian modules. The APAS has a capture ring that extends outward from the device on ISS and captures an identical device on the docking vehicle. The capture ring aligns, pulls the spacecraft together, and deploys 24 structural hooks, latching the two systems with an airtight seal.

Over the past several years, an alternative Low-Impact Docking System (LIDS) has been developed by NASA's Johnson Space Center (JSC) as a space vehicle mating device for the next generation of space exploration vehicles. In form and function, the LIDS bears some resemblance to APAS, but the two systems are not compatible. The LIDS docking device is smaller, lighter, and, most importantly in the context of this discussion, requires significantly less contact force than APAS to engage its attachment mechanisms. Given that the use of the LIDS will eliminate the need for high docking contact forces, the relative velocity required to connect two vehicles can be minimized, thus reducing overall risk.

Because the rendezvous process is complicated and multi-phase, it needs to be broken down into different operational segments with built-in pauses of the chase vehicle at the completion of each segment. These pauses provide an opportunity for the ground operations team and/or the crew to perform health and status checks on the chaser and the target vehicles prior to the next step of the rendezvous operation. The ground or the crew, if the chase vehicle is crewed, can then safely proceed to the next segment if these checks are positive. This approach provides human oversight and control of the overall rendezvous process.

In addition to many successful rendezvous and docking missions, a number of significant Russian Soyuz and Progress spacecraft near-misses or mishaps have occurred during rendezvous and docking/undocking operations. In March 1991, the Progress M-7, following a first aborted attempt to dock with the Russian Mir space station, had a near-miss encounter with the station. Rendezvous problems reoccurred later in 1991 during the process of the Mir station crew redocking its Soyuz TM-11 spacecraft to the station's rear docking port. In January 1994, the Russian Soyuz TM-17 vehicle collided twice with the Russian Mir space station vehicle upon undocking from the station. In June 1997, the Russian Progress M-34 re-supply vehicle also collided with Mir following undocking, resulting in depressurization of the Mir Spektr module. These rendezvous-related mishaps will be described below as part of the general discussion of the Russian space program rendezvous and docking history.

Gemini

In the early 1960s, even as the Mercury Program was under way, the need to close the relatively large space rendezvous and docking technology gap was clearly recognized by senior NASA management as a prerequisite to executing the envisioned Apollo Program lunar landings. Theorizing, experimenting, testing, and training on the ground alone would not provide a sufficient technical foundation upon which to build the envisioned Apollo mission rendezvous and docking capabilities. It was judged that bridging this rendezvous and docking gap would require experience directly derived from in-orbit spaceflight missions [ref. 16]. The Gemini Program was therefore structured to demonstrate and perfect the technological capabilities, mission scenarios, and operational approaches necessary for a crewed spacecraft to locate

another space platform, maneuver towards that platform in an efficient manner to effect a space rendezvous, and then perform close-in operations, including a hard docking with that platform. One of the major objectives of the Gemini Project was to rendezvous and dock with an orbiting Agena upper-stage target vehicle and perform an orbit-changing maneuver with the docked Gemini-Agena "stack" using the Agena's large propulsion system.

The specialized equipment carried on the Gemini capsule to accomplish rendezvous included radar, an optical sight, and a docking spotlight. The Agena upper-stage target vehicle was equipped with high-intensity flashing lights to allow the crew to visually track it in case of radar failure. The on-board digital computer performed terminal rendezvous maneuver navigational calculations that the crew could monitor. The physical docking of the two vehicles was accomplished with a probe and drogue mechanism.

The first-ever space rendezvous occurred on December 15, 1965, when the Gemini 6-A spacecraft conducted rendezvous and stationkeeping operations with the Gemini 7 spacecraft. This milestone event was followed shortly by the first-ever docking of two space vehicles when, on March 16, 1966, the Gemini 8 spacecraft docked with its Agena upper-stage target vehicle.

A serious anomaly occurred on Gemini 8. Shortly after completing the rendezvous and docking with the Agena target vehicle, the combined Gemini 8/Agena vehicle (or "stack") began a violent yaw motion and tumbled. Neil Armstrong, the astronaut piloting Gemini 8, undocked the Gemini capsule from the Agena, causing the capsule to roll, pitch, and yaw even more rapidly than when it was connected, approaching and possibly exceeding a rate of one revolution per second. Armstrong and David Scott managed to deactivate the Orbit and Attitude Maneuvering System (OAMS) thrusters. In a final attempt to counteract the violent tumbling, all 16 of Gemini 8's Reentry Control System thrusters were used to damp out the roll motion and stabilize the spacecraft. This recovery approach succeeded in stabilizing Gemini 8, but the control system firings consumed 75% of the fuel allocated for reentry control thruster firings. It was then discovered that one of the Gemini 8 OAMS 25-pound roll thrusters (specifically, OAMS Roll Thruster No. 8) had been firing continuously, imparting a significant disturbance torque on the vehicle and causing the tumbling. Apparently the thruster had short-circuited while being used to maneuver the Gemini/Agena stack and failed in the "stuck open" state. Although Armstrong managed to stop the tumbling of Gemini 8, had the situation been more severe it is likely the stresses would have caused crew blackout and subsequent loss of mission and crew.

Following the ground-breaking Gemini 8 success, Gemini missions 9-A, 10, 11, and 12 all conducted additional rendezvous and docking operations, in some cases using the optical sensor instead of the on-board radar. It is clear that the Gemini Program yielded invaluable on-orbit rendezvous experience for the flight crews and the mission planning/operations teams. Flight crews learned how to monitor GN&C system performance during rendezvous as well as detect and respond to system malfunctions. In reference 17, Lunney summarizes the rendezvous flight test experiences of the Gemini Program. Gemini experiences revealed how the selection of approach trajectory and lighting conditions can greatly impact rendezvous performance.

The Gemini missions showed that a combination of detailed pre-launch trajectory analysis, procedural planning, system performance evaluation, and training is necessary for mission success. The need for extensive crew-in-the-loop simulation was also shown to be a critical part of performing a successful space rendezvous. The Gemini Program paved the way for

accomplishing the goals of the Apollo Program by demonstrating that a piloted spacecraft and an uncrewed target spacecraft, each launched separately, could reliably and safety perform orbital rendezvous and docking operations.

Apollo

The Apollo mission profile called for spacecraft to have two docking maneuvers and one rendezvous maneuver in lunar orbit on every lunar landing mission. Once the Apollo spacecraft were on their way to the moon, the Command Module (CM) separated from the booster and turned around to rendezvous and dock with the LM. Then, after explorations on the lunar surface were complete, the Apollo astronauts flew the LM Ascent Stage back to lunar orbit, where they made their rendezvous with the orbiting CM.

The LM rendezvous implementation was conservative, using a Rendezvous Radar (RR) on the LM and a beacon on the CSM. The RR had a 300-mile range, range rate, and line-of-sight angle capability. Apollo proximity operations were performed under sunlit conditions.

A co-elliptic rendezvous profile was used, which had passive flyby abort capability until execution of the terminal phase intercept maneuver. The closing trajectory was designed for expected dispersions with manual control to null inertial relative line-of-sight rate and execute range-rate reduction maneuvers only. Reference 18 describes the benefits of the co-elliptic rendezvous scheme, as practiced during the Apollo lunar rendezvous operations.

Apollo spacecraft also performed on-orbit rendezvous in Earth orbit for each of the three Skylab crewed missions and for the Apollo-Soyuz Test Project.

Space Shuttle Orbiter

The Space Shuttle Orbiter has performed a relatively large number of LEO rendezvous maneuvers, among them:

- Missions to ISS.
- Several recoveries of satellites in distress (e.g., PALAPA B-2 and WESTAR VI).
- Hubble Space Telescope rendezvous and servicing missions.
- Solar Maximum Mission satellite rendezvous and servicing.
- Missions to the Russian Mir space station.

Reference 19 provides an excellent historical summary of the Space Shuttle rendezvous and proximity operations. It details the programmatic constraints and technical challenges encountered during the early phases of Shuttle mission analysis in the 1970s. Some of these technical challenges included the impacts of thruster plume impingement, processing limitations of the Orbiter's on-board computer, and propellant loading limitations. Some of the key factors influencing and constraining on-board relative navigation and rendezvous maneuver targeting are also covered, along with a description of how new flight techniques for rendezvous and proximity operations evolved to meet new Shuttle program objectives.

Initially, Shuttle Orbiter rendezvous planning assumed ground tracking would have the dominant control role. It was determined that ground tracking was not sufficiently accurate, and the GN&C rendezvous algorithm/software was tailored to allow for dispersions in position and rates (i.e., target tracking uncertainties). The Shuttle sensor had a 26-mile range using skin tracking. The Shuttle Orbiter uses a modified "stable orbit" profile instead of a co-elliptic profile. This

enables a trailing standoff relative to the target with the Shuttle in the target orbit. This is affected by executing a trailing standoff maneuver—if the maneuver were not executed, the Shuttle would execute an alternative maneuver to place it on a closing trajectory to the target with the final portion of the closing trajectory having the same characteristics of the Apollo closing trajectory. If neither of these maneuvers is executed, the "stable orbit" profile could result in the Shuttle impacting the target, depending on its relative orbit.

In later Shuttle rendezvous operations, the capability was added for computer-generated approach control instructions to the astronaut executing the commands. Shuttle crews used the Rendezvous and Proximity Operations Program (RPOP), which they ran on a laptop computer in the Orbiter cockpit, as a guidance/navigation aid and situational awareness tool from 1993 onward. By processing trajectory control sensor laser measurements to the target vehicle, RPOP output digital and graphical relative position and velocity data to assist the Orbiter pilot with meeting operational flight constraints during approach to and departure from the target vehicle [ref. 20]**.** Closing proximity operations were still manually performed, as with Apollo. Several lessons learned relating to Shuttle Orbiter rendezvous experiences are provided in reference 71.

Other Crewed Space Rendezvous Events

The Soviet Union and then the RSA made repeated on-orbit rendezvous maneuvers with Salyut, Mir, and ISS. Each crew rotation or resupply with Soyuz/Progress spacecraft required a crew-in-the-loop rendezvous with a space station. The RSA also used a technique of automated uncrewed rendezvous for resupply missions and the flights that added additional laboratories to the Mir. In this automated mode for rendezvous, the Russian crews primarily performed a monitoring function with the capability to step in during system malfunctions and provide a manual backup control role.

In addition to many successful rendezvous and docking missions, the Russian Space Program has had three notable rendezvous mishap events:

March 21, 1991: Progress M-7 Near-miss

The Progress M-7 was an uncrewed resupply vessel to the Mir space station. It attempted to dock with Mir on March 21, 1991, but missed the station by 500 meters. Ground-controlled docking was attempted again on March 23, 1991, but at a relative distance of 50 meters the docking was aborted and the Progress M-7 vehicle missed the Mir station by only 5 meters, narrowly avoiding a collision. Thereafter, it was placed in a station-keeping co-orbit with Mir while the problem was diagnosed. Finally, it successfully docked with Mir on March 28, 1991. The rendezvous problems subsequently reoccurred as the Mir crew redocked its Soyuz TM-11 spacecraft to the rear docking port on Mir's Kvant-1 module. The problem was finally traced to the Kurs rendezvous system onboard Mir. On April 25, 1991, an EVA was performed to inspect the Kurs docking system antennas, and one of the antennas was found to be missing.

January 14, 1994: Soyuz TM-17 collides with Mir

As the departing Russo-French crew conducted overflight inspection of the station, their Soyuz TM-17 spacecraft hit the Kristall module on Mir at least twice. Following the successful landing of the crew, the ground processing teams discovered a number of "souvenirs" taken by the crew from the station, which exceeded the weight limit allowed onboard the Soyuz during landing. The Russian investigation team suggested that excessive weight onboard the craft not only

endangered the crew during landing, but it could also have contributed to the problems with the attitude control system during the overflight of the station and therefore made the collision with the station more likely. Strict guidelines on allowable weight limits were imposed for future Mir station crews.

June 25, 1997: Progress M-34 re-supply vehicle collides with Mir

On June 25, 1997, the Russian Progress M-34 re-supply vehicle collided with Mir following undocking, resulting in depressurization of the Mir Spektr module [ref. 21]. At approximately 5 a.m. EDT (1:18 p.m. Moscow time), the Mir-23 crew informed controllers at the Russian Mission Control Center that the uncrewed Progress resupply vehicle had struck the station during a test of a manual redocking system and that the space station was losing pressure. Later reports from the crew indicated that during the redocking of the ship, Progress struck a solar array and a nearby radiator on the Spektr module. The collision occurred shortly before the beginning of a communication pass with Russian ground controllers. The collision caused the Spektr module to begin losing pressure. The crew closed the hatch to the leaking Spektr module, and the three crew members reported shortly thereafter that pressure was stabilizing in the rest of the station. At 5:28 a.m. EDT (1:28 p.m. Moscow time), the crew reported that the pressure in the now isolated Spektr module was continuing to drop to vacuum. At its lowest point, the normal Mir station pressure of approximately 750 mm of mercury dropped to 675 mm before it began to rise. Before the collision, station commander Vasily Tsibliev was guiding the Progress capsule to a manual docking using the teleoperated system in the core module. Tsibliev reported to the ground that the Progress had come in very fast and he could not stop it. U.S. astronaut Mike Foale said he felt the impact of the collision of the Progress with the Spektr. Foale, Tsibliev, and Flight Engineer Aleksandr Lazutkin were not injured. A Soyuz capsule attached to the Mir for use by the cosmonauts to return to Earth was undamaged. During a later communications pass at 6:53 a.m. EDT, the crew reported that the station's pressure had stabilized and that Progress had begun to separate to a safe distance from the Mir. To conserve power, the crew was told to shut down the thermal control and ventilation systems in the Kvant-2 and Kristall modules as well as the urine processing system. Other Mir systems were also powered off to conserve electricity. The station was initially spinning at approximately 1 degree per second due to the collision, but the spin had stopped and the Mir was returned to a stable configuration.

1.5.2 GN&C History for Robotic Spacecraft

Since the launch of Explorer-1 in 1958, the United States has designed, developed, and flown hundreds of robotic (i.e., uncrewed) spacecraft missions in Earth orbit (low-Earth, high-Earth, and geosynchronous), in Lunar orbit, in planetary trajectories and planetary landings, deep space trajectories, and other mission orbits and trajectories (e.g., heliocentric Earth trailing orbits and Lagrange point orbits). Most robotic spacecraft are free flyers without on-board guidance capabilities, but a select few, such as interplanetary probes, may have on-board capabilities to perform autonomous mission planning and guidance functions over the duration of their typically multi-year deep space missions. The distinction is that while the free flyers typically have an attitude control system and perhaps even an on-board navigation system, they rarely have an on-board guidance system. The robotic spacecraft serve to support mission objectives in multiple and diverse areas: Earth science, space science, meteorology, communications, navigation, remote sensing, and national defense.

Robotic Spacecraft GN&C Anomalies, Mishaps, and Failures

The majority of the U.S. robotic spacecraft missions have been successful. However, a number of them have suffered anomalies, mishaps, and total mission failures. In several cases, either the root cause or a contributing factor to the on-orbit anomaly/mishap/failure was post-facto determined to be related to some particular aspect of the engineering practices used to design, develop and/or operate the spacecraft's GN&C subsystem.

An analysis of recent on-orbit robotic spacecraft anomalies was performed by GSFC GN&C engineers in 2002 [ref. 22]**.** This analysis examined historical data recorded for satellites launched over approximately a 10-year period from 1990 through 2001. All spacecraft anomalies were considered, including those that resulted in total mission loss. Table 1.5-1 [ref. 22] lists the specific robotic spacecraft anomalies studied. The GSFC analysis concluded that a total of 35 GN&C anomalies were reported during the time period, representing 29 percent of all anomalies recorded. It should be noted that in the context of this analysis, the term "GN&C anomalies" is intended to comprehensively include anomalies due to problems with the spacecraft's on-board Attitude Control Subsystem (ACS) sensor/actuator equipment, propulsion subsystem equipment, ground operations, and/or ground software supporting GN&C mission operations.

The GN&C contribution to anomalies that result in total loss is higher, with 13 GN&C anomalies reported representing 37 percent of all anomalies resulting in total loss. This analysis also revealed that 50 percent of all GN&C anomalies occurred within the first 10 percent of the spacecraft's mission design life. Another remarkable finding of the GSFC study was that approximately 57% (20 out of 35) of all GN&C on-orbit anomalies occurring over the time frame considered were due to component (i.e., hardware) problems. Another related finding was that component problems were to blame for approximately 50% (7 out of 14) of the total mission loss events over the same time frame. This finding may be an indicator of a general trend towards reduced reliability in robotic spacecraft GN&C components. Additional anomaly/failure data gathering, analysis, and evaluation would be required to precisely determine the trend. At a minimum, however, the study results highlight a serious issue with on-orbit component behavior. This single piece of historical data is a strong motivator for GN&C engineers to work more closely with suppliers and strive for improvements in component reliability.

Table 1.5-1. Selected Robotic Spacecraft GN&C Anomaly Summary

Satellite	Launch Date	Mishap Date	Impact	Cause
Anik E2	4/5/1991	1/20/1994	Mission Interruption	Magnetic storm destroyed ACS
Aurora 2 (Satcom C5)	5/29/1991	6/1991	Shortened Life	Motor fault
Clementine	1/25/1994	5/1/1994	Partial Loss	Software error caused spin up and loss of fuel
Deep Space 1	10/24/1998	7/1999	Partial Loss	Target tracking problem due to software
Early Bird	12/24/1997	12/28/97	Total Loss	GPS unit shorted to bus draining batteries
Echostar 5	9/23/1999	7/1/2001	Mission Interruption	One of three momentum wheels fails
FUSE	6/1/1999	12/1/2001	Mission Interruption	Second of four reaction wheels fails
Galaxy 4	6/25/1993	5/19/98	Total Loss	Catastrophic attitude control failure due to SCP malfunctions
Galaxy 8i	12/8/1997	9/1/2000	Shortened Life	Three of four xenon ion thrusters fail.
GFO 1	2/10/1998	3/1998	Mission Interruption	GPS receivers fail to maintain nav state; ground-based workaround implemented
Goes 9	5/23/1995	7/7/1998	Total Loss	Taken out of service due to noisy pointing caused by lubrication starvation of momentum wheels.
GPS BII-07	3/26/1990	5/21/1996	Total Loss	3-Axis stabilization failure due to a second reaction wheel failure
Hotbird 2	11/21/1996	12/31/1996	Shortened Life	Fuel tank leak; Apogee transfer anomaly
HST	4/1/1990	11/1/1999	Mission Interruption	Fourth of six gyros fails
IMAGE	3/25/2000	3/25/2000	Mission Interruption	Nutation damper liquid immobilized by surface tension
Intelsat 801	3/1/1997	3/1997	Mission Interruption	Ground command error caused uncontrollable spin
Iridium	6/18/1997	9/1/1997	Total Loss?	Attitude control and propulsion system failure
Iridium	12/8/1997	7/17/1998	Total Loss?	Attitude control and propulsion system failure
Iridium	6/18/1997	11/2/2000	Total Loss?	Failure in orbit – fuel depletion
Iridium 5	5/5/1997	5/5/1997	Mission Interruption	Faulty wheel electronics.
Iridium 11	6/18/1997	6/18/1997	Mission Interruption	Faulty wheel electronics.
Iridium 27	9/14/1997	9/14/97	Total Loss	Thruster anomaly depleted operational fuel
Iridium 42	12/8/1997	12/8/1997	Mission Interruption	Wheel tachometer failure
Landsat 6	10/5/1993	10/5/1993	Total Loss	Satellite exploded when propulsion system pyrovalve was fired, igniting adjacent mixture.
Lewis	8/23/1997	8/26/1997	Total Loss	Design error in ACS; failure to monitor spacecraft during initial operations
Mars Climate Orbiter	12/11/1998	9/23/1999	Total Loss	Failure to use metric units in ground software trajectory models
Mars Observer	9/1/1992	8/1/1993	Total Loss	Probably due to Propulsion System rupture or power short, induced by oxidizer leaking past check valves.
NEAR	2/17/1996	12/1998	Mission Interruption	Main engine fuel burn malfunction due to on-board software limits being exceeded
Nozomi	7/3/1998	12/20/1998	Mission Interruption	Consumed more fuel than expected during Earth swingby due to thruster valve stuck partially open.
Solar A	8/30/1991	12/15/2001	Mission Interruption	Safe mode during solar eclipse, unexpected spin, loss of control
STEP 0	3/13/1994	7/19/1994	Mission Interruption	IMU (gyro) fails
STEP 2	5/19/1994	5/19/1994	Performance Loss	Noisy earth sensor affects pointing accuracy
Telstar 402	9/9/1994	9/9/1994	Total Loss	Propulsion System pyrovalve firing caused explosion
Terriers	5/18/1999	5/18/1999	Total Loss	ACS polarity error controlling magnetic torquer coil
TOMS-EP	7/2/1996	7/2/1996	Mission Interruption	Coarse Sun Sensors miswired; magnetic torque rod polarity error

Additional insight comes from an Aerospace Corporation study of satellite development practices [ref. 27], which reaffirms the need for NASA and the U.S. Department of Defense (DoD) to return to the traditional approach based on uniform design standards and rigorous

testing. This study describes a measurable decline in test rigor identified in the area of component-level "black box" thermal testing and thermal/vacuum testing. The study indicates a trend in which suppliers consistently cut back on environmental stress screening at the component level, decreasing the number of thermal cycles by as much as 50 percent to save time. The consequence, however, was an increase in component failures after the spacecraft were fully integrated and subjected to system-level thermal/vacuum testing, where the cost of the failure dramatically increases. The Aerospace study results tend to endorse an approach for accomplishing comprehensive design verification through the application of a rigorous test program starting with component–level testing at the suppliers. Therefore, emphasis needs to be placed upon the testing done at the lowest level under flight-like conditions. For example, it is only under thermal/vacuum testing that arcing is seen. A strong on-site presence to closely monitor the planning, execution, and results of these component level tests would have great value. The premise here is that an on-site engineer could identify problems/issues early enough to increase the probability of a timely and efficient resolution.

Appendix A provides a high-level summary of selected robotic spacecraft mission anomalies, mishaps, and failures. The information presented in this appendix has been extracted from final reports issued by the Mishap Investigation Board (MIB), which investigated each incident to understand what occurred and determine the incident's root and proximate causes. Among these examples are Explorer-1, Mariner-10, Voyager, Mars Observer, Landsat-6, Clementine, WIRE, Lewis, Mars Climate Orbiter (MCO), Mars Polar Lander (MPL), Terriers, TIMED, X-43, CONTOUR, and Genesis.

Individually, each of the robotic spacecraft investigation summaries provides an evidential basis for a GN&C engineering best practice; in other words, they provide valuable insights into specific GN&C-relevant examples of what can and did go wrong. Each historical "war story" has relevance to and will directly support subsequent discussions on GN&C architectural considerations, reliability issues, and specific GN&C engineering best practices for mission success.

Note that several of these examples occurred during NASA's "Faster, Better, Cheaper" (FBC) era in the 1990s. The FBC philosophy was developed and implemented by NASA with the objective of enhancing innovation, productivity, and cost-effectiveness of space missions. An objective look backward at the failure history reveals that while there were successes—and the FBC approach did allow NASA to do more with less—the overall success of the FBC model was tempered by the fact that some projects and programs over-emphasized the reductions in cost and schedule (i.e., the "faster" and "cheaper") elements of the FBC paradigm. At the same time, some of these projects and programs failed to instill sufficient rigor in risk management throughout the mission lifecycle. Actions such as these increased risk to an unacceptable level on many FBC projects, and in some extreme cases led directly to spacecraft failures. Aspects of these broad historical observations on the NASA FBC approach can be seen in the findings and conclusions reported by several of the failure investigation boards. This is especially true in the case of the MCO board's report (Appendix A).

Robotic Spacecraft Rendezvous and Docking

A number of robotic spacecraft missions have involved the demonstration or application of advanced technologies for performing space rendezvous and docking operations. In this section, a number of these robotic missions will be summarized.

Engineering Technology Satellite VII

The Engineering Test Satellite VII (ETS-VII, also called *Kiku*-7) was a JAXA (formerly NASDA) rendezvous and docking technology demonstration satellite. Launch of ETS-VII took place on Nov. 27, 1997, from Tanegashima Space Center in Japan on the H-2 launch vehicle. ETS-VII was placed in a 96-minute period circular orbit with an altitude of 550 km and an inclination of 35°. A further payload on this flight was the TRMM spacecraft, a joint mission of NASA/NASDA. ETS-VII experienced an attitude stability problem on Nov. 30, 1997, that was corrected.

The overall mission objectives were to conduct space robotic experiments and demonstrate their utility for uncrewed orbital operation and servicing tasks. In the rendezvous-docking experiment, the Chaser satellite was to conduct rendezvous and docking with the Target satellite by both automatic and remotely piloted controls. Propulsion anomalies appeared in the initial docking attempt, but measures were taken to minimize their effects. During an experiment in August 1998, the two satellites had approached to a distance of 145 meters, whereupon the Chaser satellite experienced an attitude control anomaly and transitioned to a safe mode. As a result, the docking was not accomplished. Both satellites were placed in station-keeping mode 1.2 kilometers apart at the orbital altitude of 550 km.

By revising onboard software, a new thruster combination was selected that did not require the Z-axis thruster that had caused the firing problems. The rendezvous-docking experiment was conducted successfully two times with the Chaser satellite being both automatically and remotely piloted. The first docking was completed at 20:43 (JST) on October 27, 1999. On December 15, 2000, NASDA acquired data of rendezvous, docking, and communication using data relay satellites in the final experiment. In these experiments, a RendezVous laser Radar (RVR) was used as the primary navigation sensor during the final approach phase (over the range of relative distances from 500 meters to 2 meters). The RVR functioned properly, and its performance characteristics in terms of measurement accuracy, optical propagation, and acquisition/tracking operation, satisfied the requirements. The experimental results showed that RVR was effective for autonomous rendezvous docking. With the completion of this final test, the on-orbit experiments for ETS-VII, conducted over a two-year period, were successfully accomplished.

Near Earth Asteroid Rendezvous

The Near Earth Asteroid Rendezvous (NEAR) mission is the first launch in the Discovery Program, which was a NASA initiative for small planetary missions with a maximum 3-year development cycle and a cost capped at $150 million for construction, launch, and 30 days of operation. The primary objective of the NEAR mission was to rendezvous with and achieve orbit around the near-Earth asteroid called 433 Eros in February 2000. Eros was selected as the rendezvous target since its orbit could be well determined prior to the actual rendezvous. Once inserted into orbit around Eros mission plans called for NEAR to then study the asteroid for approximately one year at altitudes as close as 24 Km to the asteroid's surface. The NEAR

mission was designed and developed by The Johns Hopkins University Applied Physics Laboratory (JHU/APL) in Laurel, Maryland. The NEAR spacecraft was built and launched in 29 months. The challenging mission requirements dictated the use of a three-axis active GN&C subsystem to control the spacecraft's attitude nominally using momentum wheels and periodically using thrusters when performing trajectory-altering maneuvers [ref. 23]. The guidance algorithms were based on stored orbit data and attitude determination was based on a filtered combination of star camera and inertial sensor inputs. The laser rangefinder used as the proximity rendezvous sensor was a reduced-scale and more reliable advanced technology version of the rangefinder flown on the Naval Research Laboratory Clementine mission.

Also of note, the spacecraft designers developed and implemented a reliable and comprehensive safing system that had one Earth-Safe mode and two Sun-Safe modes of operation. One place "new technology" was employed on NEAR was in the system of software autonomy rules developed to maintain the spacecraft in a safe and healthy state between infrequent contacts with Earth through the Deep Space Network, especially during the long cruise phase to the Eros asteroid target [ref. 24].

The spacecraft was launched on February 17, 1996, into a rendezvous trajectory with Eros using a Delta-II booster. The NEAR mission designers at JHU-APL employed two-year Delta-VEGA (Delta-V and Earth Gravity Assist) trajectory technique to accomplish the successful asteroid rendezvous [ref. 25]. The first relatively large deep-space maneuver to significantly alter the spacecraft trajectory was performed in July 1997 using the spacecraft's large bipropellant velocity adjust thruster. In January 1998, the spacecraft swung by Earth for a gravity-assist maneuver. Numerous relatively small trajectory correction maneuvers (TCMs) were also performed during the flight to Eros. Thruster commanding for TCMs was performed under ground control only, with parameters loaded into the on-board control processor in advance and verified prior to the maneuver. The operational philosophy used by the NEAR mission managers was a conservative "better safe than sorry" one in which no propulsive maneuvers with critical timing were to be performed. In addition, this philosophy dictated that if anomalous dynamic behavior occurred during a propulsive maneuver, the thrusters would be rapidly shut down, the problem corrected, and the maneuver re-scheduled. This type of conservative operational approach could be implemented for NEAR because of the flexible and robust nature of its mission design as well as the fact that the spacecraft carried a very large propellant margin.

The initial close pass flyby of Eros occurred in December 1998. An anomaly occurred during the first propulsive "encounter" maneuver, during which the burn was aborted within a fraction of a second from bi-propellant initiation and the telemetry signal from the spacecraft was lost 37 seconds following the burn abort. Fortunately, contact with the spacecraft was reestablished about 27 hours after the aborted burn; the spacecraft was determined to be stable in its Sun-safe mode controlled by a backup processor. It was subsequently determined that 96 meters/second of propulsive Delta−V capability was lost as a result of this burn anomaly. This NEAR anomaly is discussed in detail in Appendix A. Once this anomaly was investigated and the problem was resolved, the second DSM was successfully performed in January 1999. A sequence of propulsive rendezvous maneuvers was subsequently performed to reduce the relative velocity between the Eros target asteroid and the NEAR spacecraft to only a few meters per second leading to their eventual rendezvous in February 2000. NEAR was inserted into an initial 323 x

370 km orbit with a period of 27 days. The spacecraft later maneuvered to a 100 x 200 km orbit around Eros in April 2000.

The spacecraft spent the next year performing its science mission orbiting Eros, returning spectacularly detailed pictures of the surface and assessing its size, shape, mass, magnetic field, composition, and structure. The periapsis of the NEAR orbit dropped as low as 24 km above the asteroid surface during this period.

On February 12, 2001, the NEAR spacecraft touched down on asteroid Eros after transmitting 69 close-up images of the surface during its final descent. This event marked the end of the 5-year NEAR mission. In summary, NEAR was the first spacecraft to rendezvous with, orbit and then land on a small body.

Demonstration of Autonomous Rendezvous Technologies

On April 15, 2005, the Demonstration of Autonomous Rendezvous Technologies (DART) spacecraft was launched from the Western Test Range at Vandenberg Air Force Base, California. DART was designed to rendezvous with and perform a variety of maneuvers in close proximity to the Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM) satellite, without assistance (autonomously) from ground personnel.

During the actual DART mission, all went as expected throughout the launch and early orbit phases. The vehicle successfully completed its rendezvous phase as well, placing itself into a second staging orbit about 40 kilometers behind and 7.5 kilometers below MUBLCOM, even though ground operators began to notice an irregularity with the navigation system.

When DART began its transfer out of the second staging orbit to begin proximity operations, ground operators observed that the spacecraft was using significantly more fuel than expected for its maneuvers. It became clear that the mission would likely end prematurely because of exhausted fuel reserves. Because DART had no means to receive or execute uplinked commands, the ground crew could not take any action to correct the situation.

During the series of maneuvers designed to evaluate Advanced Video Guidance Sensor (AVGS) performance, DART began to transition its navigational data source from the GPS to AVGS as planned. Initially, the AVGS supplied only information about MUBLCOM's azimuth (angular distance measured horizontally from the sensor boresight to MUBLCOM) and elevation relative to DART. However, as DART approached MUBLCOM, it overshot an important position in space that would have triggered the final transition to full AVGS capability. Because it missed this critical waypoint and the pre-programmed transition to full AVGS capability did not happen, the AVGS never supplied DART's navigation system with accurate measurements of the range to MUBLCOM. Consequently, DART was able to steer towards MUBLCOM, but it was not able to accurately determine its distance to MUBLCOM. Although DART's collision avoidance system eventually activated 1 minute and 23 seconds before the collision, the inaccurate perception of its distance and speed in relation to MUBLCOM prevented DART from taking effective action to avoid a collision.

Approximately 11 hours into what was supposed to be a 24-hour mission, DART detected that its propellant supply was depleted and began steps to initiate a series of departure maneuvers. Although it was not known at the time, DART had actually collided with MUBLCOM 3 minutes and 49 seconds before initiating departure. MUBLCOM did not appear to experience significant

damage, and the impact actually pushed it into a higher orbit. Then, shortly after the collision, DART determined that it was nearly out of maneuvering fuel and initiated its pre-programmed departure and retirement maneuver. DART's departure and retirement phase proceeded per the original plan, and MUBLCOM regained its operational status after an automatic system reset that resulted from the collision.

Because DART failed to achieve its main mission objectives, NASA/HQ declared a "Type A" mishap and convened an MIB to perform a detailed investigation. The DART MIB initiated its investigation activity during the week of April 18, 2005, and completed its activities approximately five months later with the submittal of its final report. The MIB's final report clearly identifies and explains the causes of the DART mishap and provides a comprehensive set of findings and recommendations.

DART was a one-time project. Because of this, the MIB did not propose specific design changes for the DART spacecraft. The formal mishap report contains detailed recommendations for the root causes that should prevent similar mishaps in the future. A summary of the root causes and recommendations identified by the DART MIB is provided in Appendix A.

XSS-11

The U.S. Air Force Experimental Satellite System-11 (XSS-11) micro-spacecraft was launched on April 11, 2005, from Vandenberg Air Force Base, California, on a Minotaur booster into an orbit with 800 km altitude. The mission objective was to utilize a small 100kg spacecraft to explore a range of military functions, including 1) the demonstration of manual rendezvous and proximity operations; 2) the validation of an autonomous process for the planning and execution of space rendezvous; 3) the refinement of tools and operational concepts for space rendezvous; and 4) the characterization of the performance impact of spacecraft position and velocity uncertainties on rendezvous operations. The XSS-11 system was developed under the sponsorship of the U.S. Air Force Research Laboratory's (AFRL) Space Vehicles Directorate at Kirtland Air Force Base (New Mexico). The XSS-11 mission leveraged the success of a precursor mission called XSS-10. The XSS-10 spacecraft performed a 20-hour mission in January 2003 during which it performed proximity operations and inspection of the second stage body of the Delta-II booster that launched it into orbit. These small and affordable XSS-10/11 micro-spacecraft missions made significant technical contributions by demonstrating the technology needed for the critical functions of autonomous mission planning, rendezvous, and proximity operations. It was foreseen that these functions would be routinely required in the future to expand Air Force space control operational capabilities. Initially, the XSS-11 spacecraft successfully demonstrated rendezvous and proximity operations with the expended upper stage of its Minotaur booster. During the remainder of its 12-18 month mission life, XSS-11 conducted rendezvous and proximity maneuvers with several U.S.-owned dead or inactive resident space objects near its orbit. The AFRL reported that, as of May 2006, the XSS-11 spacecraft had accomplished 50 rendezvous engagements, more than 300 natural-motion circumnavigations of targets, and over 1,200 hours of proximity operation. Some high-level operational lessons learned from the XSS-11 mission include 1) Expect that proximity operations will take longer than expected; 2) Anticipate off-nominal conditions and pre-plan appropriate recovery procedures; 3) Establish a team responsible for mission safety; 4) Monitor in real-time the GN&C performance and fault management software status; and 5) Understand the impacts of thruster performance on rendezvous and proximity operations. In summary, during its mission,

the successful flight of the XSS-11 spacecraft contributed to the evolution of technologies to efficiently plan, evaluate, and safely oversee not only a variety of autonomously conducted space rendezvous and proximity operations, but also those needed for a new class of affordable micro-spacecraft platforms that would lower launch costs and extend the capabilities of future space missions. The XSS-11 system was rapidly developed over a period of slightly more than 3 years: from initial concept definition to launch took 39 months. The mission had a total program cost, including launch and mission operations, of approximately $80 million. Lockheed-Martin Astronautics (Colorado) served as the XSS-11 systems support contractor.

Orbital Express

The Orbital Express Demonstration System (OEDS) flight demonstration project was established and sponsored by the Defense Advanced Research Projects Agency (DARPA) to develop and validate key technologies required for cost-effective servicing of next-generation spacecraft. A Boeing-led contractor team built the two-spacecraft OEDS which was launched 8 March 2007, aboard an Atlas V launch vehicle, to begin a four-month on-orbit mission. OEDS included the Autonomous Space Transport Robotic Operations (ASTRO) Servicing spacecraft, built by Boeing Advanced Network and Space Systems and the Next Generation Serviceable Satellite (NEXTSat), serving as a client vehicle, built by Ball Aerospace Corporation. The two vehicles were launched together in a mated configuration. The low earth orbit test flight demonstrated autonomous rendezvous and capture (AR&C) functions using advanced GN&C sensor, guidance, and relative navigation hardware and software.

As described in reference 63, during the course of six unmated scenarios, the ASTRO spacecraft demonstrated completely autonomous rendezvous and capture (AR&C) of the NEXTSat from ranges of 10 meters to hundreds of kilometers using advanced sensor, guidance, and relative navigation hardware and software technologies. NEXTSat capture was performed in two ways, via direct capture, using a three-pronged soft capture mechanism, and freeflyer capture, using a robotic arm.

The Orbital Express mission accomplished numerous first-of-a-kind activities in space, including:

1) Autonomous capture and servicing of a client spacecraft;
2) Fully autonomous capture of a free flying vehicle;
3) Autonomous component transfer using a closed-loop servo-vision system;
4) Fully autonomous on-board navigation and guidance to approach and stationkeep within 10 cm of a client spacecraft using a passive vision system;
5) Fully autonomous “soft” capture of a spacecraft while stationkeeping;
6) Fully autonomous transfer of hydrazine propellant from one vehicle to another on-orbit with US technology.
7) Transfer of a battery and a computer avionics unit between spacecraft on-orbit.

ASTRO’s Autonomous Rendezvous and Capture Sensor System (ARCSS) used onboard visible, infrared and laser rangefinder sensors to provide real-time data and imagery to an onboard sensor computer. As part of the OEDS project Boeing-developed the Vision-based Software for Track, Attitude and Ranging (Vis-STAR) software, executing on the sensor computer, provided

precision real-time client bearing, range and attitude as needed, from ranges of over 200 km to soft capture. All the onboard sensor algorithms were successfully demonstrated, including algorithms for long-range tracking, silhouette and edge tracking of the extended target against space and Earth backgrounds, and docking target plate track against NEXTSat vehicle clutter.

Reference 63 summarizes in detail the results of the on-orbit performance testing of the ARCSS (Autonomous summarizes the ARCSS and Vis-STAR on orbit performance. Elements of this advanced GN&C technology demonstrated on the Orbital Express mission are being infused into the Starliner CST-100 Reusable Spacecraft Capsule being developed Boeing to support rendezvous and docking functions.

ESA Automated Transfer Vehicle

The Automated Transfer Vehicle (ATV) is a major European contribution to the ISS Program. In combination with the Ariane 5 booster, the 20.5 ton, 8.5 meter-long ATV will enable Europe to transport scientific equipment, general supplies, water, oxygen, and propellant to the ISS. This robotic re-supply spacecraft will physically dock and mate to the ISS Service Module (the Russian segment). The ATV's 45 meter^3 pressurized module will carry 8.5 tons of cargo to the ISS. Up to 4 tons can be propellant for ATV's own 490-Newton main liquid bi-propellant engines to perform orbital reboost of the ISS at regular intervals to compensate for atmospheric drag effects.

The ESA plans to launch the first ATV flight model, named "Jules Verne," on its rendezvous and docking mission to the ISS in mid-2007. The ATV is currently undergoing final integration and space environmental tests at ESA's test facilities in Noordwijk, the Netherlands.

The ATV GN&C hardware suite consists of two star trackers, a GPS receiver, four Videometer optical rendezvous sensors, and 28 220-Newton liquid bi-propellant attitude control and orbital braking thrusters. There is also an S-band radio frequency link between the ATV and the ISS for proximity operations. A monitoring and safing unit (MSU) is employed on the ATV to detect a critical failure or an unsafe situation. The function of the MSU is to isolate the ATV's nominal system and then command a Collision Avoidance Maneuver (CAM). This brings the ATV on a safe trajectory within the monitoring corridor towards the ISS. Once the CAM is completed, the MSU would point the ATV towards the Sun, thus ensuring sufficient power from the solar panels during the "survival" mode that the vehicle then enters. Additionally, a CAM can also be manually commanded either by the ATV Control Center or by the ISS crew upon their detection of any abnormal behavior.

The ATV program has expended significant effort to validate the platform's rendezvous and docking system's sensors and software. The ATV rendezvous and docking system has recently completed a significant development milestone. A series of qualification tests were conducted on the ATV's integrated flight sensor/flight control software system. These tests utilized a sophisticated multi-DoF relative motion simulation hardware and software testbed facility near Paris, France. Closed-loop end-to-end integrated rendezvous and docking system tests which replicating the ATV's final approach to the Russian docking port on the ISS were performed. Each approach was conducted in steps, in real-time, over several hours with the mobile platform advancing at an extremely slow pace. A mobile platform was controlled to replicate the precise relative motion that the ATV and the ISS were expected to experience during approach, from a range of 250 meters to within docking contact conditions. On the platform, a set of passive

rendezvous targets (retroreflectors), identical to the ones installed on ISS, faced the ATV rendezvous sensor package mounted on an articulated robotic arm. This platform replicates the closing motion between ATV and ISS, and the robotic arm replicates the relative rotation and lateral motion between the two vehicles. To make this rendezvous system testing as realistic as possible, a full-scale mockup of the aft end of the ISS Service Module was placed on the test facility's moving platform. This mockup included the Russian docking port (including the Russian-made thermal blankets) and the retro-reflective targets.

These tests also were to obtain a realistic performance characterization of the ATV's Videometer sensor flight hardware capabilities, both in the in acquisition phase and in the targeting phase of the rendezvous. During the simulated rendezvous engagement, the Videometer tracking performance of the ISS retroreflectors was monitored. The function of the Videometer is to process images of its emitted laser beam as reflected back to the ATV by the passive retroreflectors installed on the ISS next to the Station's Russian docking port. During these tests the Videometer output data was input directly to the ATV flight control system software in a closed-loop manner.

JAXA H-II Transfer Vehicle

The JAXA H-II Transfer Vehicle (HTV) is an uncrewed re-supply space vehicle similar to ESA's ATV, which transports cargo from the Tanegashima Space Center to the ISS. The HTV will deliver daily goods such as water, food and clothing, and experimental equipment to the Japanese Experiment Module after the completion of ISS assembly.

The HTV is an uncrewed orbital transfer vehicle that measures 10 meters in length and 4.4 meters in maximum diameter. The HTV vehicle weighs 16.5 tons and carries a 6-ton payload to the ISS in logistic carriers. At the rear of the HTV are an avionics module that accommodates navigation electronics and a propulsion module that supports the vehicle's rendezvous with the ISS.

After the insertion to the orbit by a heavy-lift version of the H-IIA launch vehicle, the HTV will perform rendezvous maneuvers using position data from the relative GPS navigation system and the Rendezvous Laser Radar. HTV uses a rendezvous algorithm, which was validated on the Engineering Test Satellite-VII (ETS-VII) technology demonstration satellite. The HTV has been designed for a solo flight duration of about 100 hours. An S-band radio frequency (RF) communications system link is also established between the HTV and the ISS when the relative distance between the two craft closes to within 23 km. This communication link allows the two-way flow of mission critical data and commands during HTV rendezvous and proximity operations. The link transmits the GPS data from the ISS to the HTV along with safety- critical ISS crew commands to the HTV. This RF link provides range and range rate measurements to monitor the HTV flight path as it approaches the ISS. The ISS will also receive HTV state-of-health telemetry data over this link.

The HTV halts at a predetermined region called Berthing Box, some 10 meters below an ISS berthing port. Unlike the ATV, the HTV will not have a docking capability. Instead, once the HTV is maneuvered into Berthing Box, the Canadian Space Station Robotic Manipulator System robotic arm will then grapple/capture the re-supply craft and position it to one of the ISS docking ports. This HTV berthing method was devised by mission designers to lower the risk to the crewmembers onboard the ISS in the event of a HTV malfunction/anomaly. The HTV has been

designed to remain docked with the ISS for about 30 days. After the completion of its re-supply mission to ISS, the HTV will self-destruct when it re-enters the atmosphere.

As of mid-2006, an HTV prototype had been developed at the Tsukuba Space Center. This prototype will be subjected to thermal, acoustic and vibration environment tests to verify and qualify the vehicle's basic design. The HTV is scheduled to be launched by an augmented H-IIA, the H-IIB launch vehicle, which is currently under development in Japan, in 2008.

1.5.3 Comparison of GN&C DDT&E Practices for Human-Rated and Robotic Spacecraft

An historical comparison of the GN&C systems used for human-rated spacecraft versus those flown on robotic spacecraft reveals a number of similarities and differences. From a functional viewpoint, one can see that the GN&C for both crewed and robotic spacecraft must operate and perform in many of the same mission phases. For example, although the robotic spacecraft GN&C is not typically fully operational, or even powered on, during launch and ascent it must survive the same stressful environmental rigors of a powered boost phase as a crewed spacecraft's GN&C. Some robotic spacecraft have mission requirements that require their GN&C subsystem to perform some or all of the same functions that would be demanded of a crewed spacecraft. The history shows some robotic missions required the GN&C system to compute and perform propulsive orbit/trajectory maneuvers for the vehicle to escape Earth orbit in order to reach the Moon, the planets, the Earth-Sun Lagrange points or other regions of scientific interest. Also some robotic missions have required the GN&C to support planetary entry, descent, and landing (EDL) operations (e.g., the Mars Exploration Rover landings in 2004), including, in a few cases, a fully autonomous precision soft landing on potentially hazardous terrain (e.g., the Surveyor lunar landers in the mid-1960s and the Viking Mars landers in the mid-1970s). Still other types of robotic missions necessitated a capability for a planetary orbit rendezvous (e.g., the Mars Sample Return mission).

Generally speaking, the generic end-to-end GN&C DDT&E process portrayed in Figure 1.4-1 can be applied equally well to robotic and crewed spacecraft GN&C design and development. Very strong similarities exist in the type of GN&C navigation and attitude sensors used on both classes of platforms. There is some level of similarity as well in the type of actuators employed, as both crewed and robotic spacecraft typically use the same type of vernier reaction control thruster technology to generate both attitude control torques and small orbit/trajectory correction forces. However, some types of attitude control actuators typically flown on NASA robotic spacecraft (e.g., small reaction/momentum wheels and magnetic torquers) have not been used on U.S. human-rated spacecraft to date. Likewise, the type of very large CMG actuator currently flying on the ISS would rarely, if at all, be used on a NASA robotic spacecraft. Designers of both types of GN&C systems must each deal with the reality that there is now, primarily due to industry coalescence, only a small number of third-tier GN&C component vendors offering a limited product line of COTS hardware. The detailed GN&C engineering design steps and analysis methodologies (i.e., controller stability analysis) as well as many of the associated software-based tools used to perform analysis are the same in both cases.

There are many fundamental differences between the two types of GN&C systems. The primary difference is the level of fault tolerance required on human-rated spacecraft to ensure the GN&C system-level reliability supports the satisfaction of the top-level crew safety requirements. In particular, the GN&C systems for crewed spacecraft must satisfy the safety and reliability

requirements as defined in each project's Human-Rating Plan. This plan lists requirements for, among other things, design criteria (including software), test and verification, system safety/reliability engineering, and human factors engineering. These project specific requirements are tailored and derived from the top-level NASA Program Requirements (NPR) Human-Rating Requirements Document. (i.e., NPR 8705.2). Details may vary but it is highly likely that all future U.S. human-rated spacecraft will have a high-level two-fault tolerant fail operational/fail safe requirement that will flow down to the GN&C designer from the NPR 8705.2 governing document.

The point is that the designer of a GN&C system for a human-rated system must always keep the physical safety of the crew foremost in mind. Early on, the designer should build checkpoint steps into the GN&C design process that will help ensure that all conceivable GN&C failures/malfunctions that would pose a crew hazard are recognized and adequately addressed. If the specific fault tolerance requirements cannot be met, then the GN&C designer will need to adopt a "Design for Minimum Risk" approach. The fundamental overriding objective is to ensure the highest probability of safe crew return for all operation modes and flight regimes in which the vehicle is expected to fly. Early trade studies to define and select the safest GN&C system architecture are required to accomplish this objective without any major GN&C redesign over the spacecraft's life cycle.

The GN&C engineer on a human-rated spacecraft development project must clearly understand which aspects of the mission are "Mission Critical" (1-fault tolerant) and which are "Crew Critical" (2-fault tolerant). This mission criticality versus crew criticality drives the fault tolerance that must be embedded in the GN&C system on a human-rated spacecraft. Building in sufficient fault tolerance for crew safety is a very fundamental distinction and it is an aspect of system design that the robotic spacecraft GN&C designer is never concerned with.

Fault tolerance is a deep multidisciplinary subject involving spacecraft avionics (e.g., flight processors, remote interface units and the connecting data buses), FSW, GN&C, human factors and perhaps other technical areas in some cases. In practice, fault-tolerant design is based on redundancy, and it should start at the spacecraft architectural level and flow down to the GN&C system. The design of fault-tolerant systems for human-rated aerospace systems is beyond the scope of this discussion but it is insightful to at least mention one relevant lesson learned from the Space Shuttle Program. Usually some form of voting is employed in a fault-tolerant system. Voting schemes face a dilemma, however, of identifying a failure among three or two identically redundant avionics units (e.g., an IMU). In the case of the Shuttle Orbiter, which flew three identical zero-fault tolerant IMUs, it was relatively straightforward to identify (i.e., vote out) the first IMU failure but the task of identifying the failure of a second IMU, out of the remaining two healthy IMUs, was problematic. This condition is sometimes referred to as the "man with two watches doesn't know what time it is" syndrome. In general, the need to identify a second failure comes directly from the high-level mission requirement to be two-fault tolerant. RM FSW was therefore developed for the Orbiter to resolve the dilemma of identifying a second IMU failure between two healthy units. This highly complex RM development process for the Orbiter resulted in a large number of source lines of code and a costly V&V effort to certify the RM software costs. There were also significant life-cycle costs associated with updating, maintaining and re-certifying for flight the Orbiter's RM FSW over the multi-year Orbiter operation period. It is commonly understood that the Space Shuttle Program's decision to employ the RM FSW

approach was initially based upon the results of a tradeoff between the cost/mass/power impact of flying an additional (fourth) zero-fault tolerant IMU identical to the other three in the avionics design. In retrospect, it appears the costs associated with the development and maintenance of the RM FSW far outweighs the cost of an additional IMU. Another factor to be highlighted here is the complexity of the RM FSW, which created a barrier to flight operations staff to learn and fully understand its internal computations and output behaviors. The potential drawbacks of using software (with its relatively high maintenance costs over the mission life cycle) instead of hardware to efficiently and affordably identify the second failure within a family of identical GN&C hardware units is the lesson to be learned here from the Orbiter RM experience. This experience also reinforces the point that features of the selected GN&C architecture will have long-term ramifications throughout the spacecraft's lifecycle; these features should be carefully considered and well supported with thorough trade studies.

A major difference between the two types of GN&C occurs in the area of contingency planning and contingency response. In both the robotic and crewed mission applications, the GN&C system must be designed to operate under routine (nominal plus reasonable uncertainty factors) flight conditions. However, the human-rated spacecraft GN&C system must also be designed with sufficient functional capabilities to ensure the safety of the crew under the extreme flight conditions when severe spacecraft and/or launch vehicle degradations, malfunctions and failures may occur. An abort strategy must be formulated to dictate the system response and the specific actions to be taken to remove the spacecraft (with its crew) from an intolerably unsafe and possibly hazardous dynamic state. Abort planning will first consider those phases of the mission where risk levels are the highest. For NASA human-rated crewed spacecraft, these high-risk phases occur at the beginning and the end of each mission. That is to say, they occur during the launch event itself (booster ignition), during the powered flight ascent trajectory into the initial mission orbit about Earth, and during the EDL phase of the mission. Unsafe conditions could arise from many problems that span the entire mission envelope. A launch vehicle propulsion system problem will, after attempting all possible pre-abort options, trigger an abort. Future human-rated spacecraft will need some form of on-board autonomous "abort manager" software to rapidly detect an anomalous condition during launch, ascent, rendezvous, and/or the EDL phases and take steps to either resolve the anomaly (e.g., by swapping out a "bad" IMU for a "good" IMU) or, where possible, to trigger the initialization of a pre-planned abort mode. Although the details are not within the scope of this particular GN&C discussion, it should be mentioned that a highly robust and reliable fault-tolerant processing capability must be provided, especially during these brief but stressful mission events. During the EDL phase, for example, there is no time to re-boot flight processors in the face of a computing fault and/or failure. Rather, the fault-tolerant processing system should, in a manner that is transparent to the GN&C system, manage (e.g., detect, mask, contain, recover, or reconfigure) any computing faults and/or failures. Aborts during launch and ascent will prematurely terminate the mission to return the crew safely to Earth. The designers of robotic spacecraft GN&C systems never specifically consider this type of launch-related abort planning and design implementation.

It is true that robotic spacecraft GN&C designs do not universally have "abort modes" of operation, but it is very typical for the GN&C system on a robotic spacecraft to include one or more safe-hold modes. During routine on-orbit operations, it is not uncommon for robotic spacecraft to failover to a degraded-performance safe-hold mode in the face of an on-board GN&C anomaly that cannot be directly resolved on-board with pre-determined sensor, actuator,

processor, and/or software reconfigurations triggered by resident FDIR FSW logic. In these cases, the robotic spacecraft remains in the offline power/thermal safe configuration in an orientation that allows for periodic (at worst) or preferably continuous telemetry, tracking, and command communications with the ground. Under certain fault or failure situations, a robotic spacecraft may stay in its degraded GN&C performance safe-hold mode for days and perhaps weeks until such time as the ground operations team can diagnose and identify the cause of the anomaly and take corrective action to bring the vehicle back on-line with full GN&C performance to resume its normal mission operations.

NASA's next generation of crewed spacecraft would benefit from having safe haven modes of operation, analogous to the safe-hold modes used on robotic spacecraft, in addition to a comprehensive set of abort mode capabilities. For example, it would be prudent to have a safe haven attitude control mode in place for those flight periods where the crew is not providing continuous watch. This capability might be particularly useful on missions with a long-endurance cruise phase.

There could possibly be abort scenarios where the mission is continued but with highly altered and much less ambitious objectives than originally planned. In these cases, an abort could result in the spacecraft being temporarily placed, either automatically or via crew command, into a safe haven mode. An example of this can be found within the context of space rendezvous. The determination that a chaser spacecraft is on a collision course with the target spacecraft during rendezvous and docking operations should trigger an abort. A possible GN&C system response to such an abort occurring during the terminal phases of a rendezvous would be to initiate a chase vehicle orbital maneuver to enter a nearby collision-free safe orbit and to then transition the spacecraft into a safe haven mode until the anomaly is resolved and the GN&C system recovery completed. This type of human-rated spacecraft on-orbit contingency and abort planning, as well as the functional implementation of safe haven modes, is not unfamiliar to robotic spacecraft GN&C designers.

Robotic spacecraft GN&C system designers often exploit the advantages of flying dissimilar flight hardware. There are many examples of this. Digital fine Sun sensors are often used to back up star trackers for precision attitude determination. Magnetometers can be used for backup attitude determination, and thrusters can be used in place of magnetic torquers to unload excess reaction wheel momentum. Separate and dissimilar processors are used to host and execute digital safe hold mode control laws.

Designers of human-rated spacecraft GN&C systems should consider employing sensor and actuator dissimilarity to, at a minimum, provide the crew with backup manual vehicle control options in a safe haven mode. Implementing this backup functionality would require the architecting, early in the DD&TE process, of a dissimilar set of flight control software algorithms running on a dissimilar processor with sensor feedback from a dissimilar IMU and some associated panel displays and hand controllers.

There are two fundamental benefits of having dissimilar GN&C hardware and software on either a robotic or human-rated spacecraft. Firstly, dissimilar GN&C hardware is of great value in fault detection and isolation. The correct diagnosis is more certain when a diverse set of dissimilar hardware and/or software is used to perform FDIR functions on the spacecraft. Secondly,

dissimilar GN&C hardware and software can be brought on-line and into service in support of the recovery process.

Finally, consider that along with the advantages of flying dissimilar GN&C equipment comes some finite level of incremental cost and risk increase. The dissimilar hardware selected should be high- Technology Readiness Level (TRL) proven components, not advanced technology items. Even so, it is quite likely the components will require different mechanical, electrical, and software interfaces, have different operational constraints, and require their own dedicated test sets and test procedures. Furthermore, if these dissimilar units are being added to an existing baseline architecture, the GN&C designer will have to justify any necessary increase in mass and power resource allocation. Also, these dissimilar GN&C devices will have their own unique operational nuances and idiosyncrasies that will need to be characterized and understood. In summary, it is advisable for GN&C designers to carefully consider the full range of the tradeoff between using dissimilar GN&C hardware units as an alternative to a non-diverse redundancy approach using multiple identical copies of a single given unit.

Some, but not all, of the other differences between human-rated and robotic spacecraft GN&C systems are:

1. Generally speaking, NASA and its various contractor teammates have far more experience in the DDT&E of GN&C systems for robotic spacecraft than for crewed spacecraft. A wide variety of mission-unique robotic spacecraft GN&C architectures are designed, implemented, and flown each year. A conservative estimate, based upon the average number of new flight project starts over the past 20 years, indicates that NASA performs or sponsors the design and development of three to five new robotic spacecraft GN&C systems per year. In comparison, NASA and its contractors have designed, developed, and flown only two new human-rated GN&C systems, one on the Space Shuttle and one on the ISS, since the termination of the Apollo and Skylab Programs in the 1970s. The level of complexity, specific sensor and actuator components, FSW, level of on-board autonomy and size, and scope of the associated ground systems and ground operations teams have all varied depending on the nature of the robotic mission requirements. The result is that NASA and its contractors have a substantial and diverse GN&C engineering experience base for robotic spacecraft applications.
2. The GN&C systems on most human-rated spacecraft to date were required to operate over mission durations on the order of weeks to months. The one obvious exception to that is the ISS GN&C system, elements of which (e.g., the CMGs) can be replaced. The longest mission durations for future lunar exploration spacecraft will be on the order of months, not years. Typically robotic spacecraft missions are of multi-year duration and can be as short as 2-3 years or as long as 10-15 years. The GN&C system is expected to reliability function over that multi-year period. The GN&C systems of robotic spacecraft are not typically designed to be serviced in-flight. The Hubble Space Telescope is the one obvious exception to that general rule. A recent trend is however to include certain robotic spacecraft design features on client spacecraft that specifically support potential cooperative in-flight servicing. These feautres include, among others, laser retro-reflectors, visual and infrared fiducial markings, berthing features, robotic grapple fiducials and fixtures, cooperative fluid ports, and free drift ACS Mode.

3. Unlike the case for robotic spacecraft, it is likely that future human-rated spacecraft will be reused multiple times over a multi-year operation period. The physical, economic, and safety-related impacts of refurbishing, servicing, and/or replacing GN&C hardware on the ground after each mission must be considered early in the GN&C design process. Robotic spacecraft are virtually never reused to fly multiple missions, so the ground refurbishment, servicing, and/or replacement of GN&C equipment are extremely rare occurrences. A notable exception to this general rule was the Solar Maximum Mission (SMM) Modular Attitude Control System (MACS) that was returned from space by the Orbiter as part of the 1984 SMM repair mission, refurbished and then flown again on the Upper Atmospheric Research Satellite (UARS).
4. Labor-intensive V&V costs to regression test and recertify any modified GN&C flight hardware and FSW are more burdensome for human-rated spacecraft GN&C applications than for robotic spacecraft GN&C.
5. System mass and power are two commodities carefully allocated and closely managed on both crewed and robotic spacecraft but the essential electrical power resource required to operate the GN&C is typically more scarce on robotic spacecraft. This results in different GN&C system architectural approaches. Power constraints on robotic spacecraft often preclude the flying of multiple copies of identical GN&C hardware units. Given these power constraints, robotic spacecraft GN&C subsystems are therefore often designed with a minimally redundant set of sensor/actuator hardware (e.g., 4-for-3 redundancy at the individual inertial sensor level) as compared to the Shuttle Orbiter, which flies with a complement of three identical IMUs.
6. The “cockpit panel” displays, monitors and alarms, as well as the hand controllers used for piloting inputs, which are typically used on crewed spacecraft are non-existent on robotic spacecraft.
7. For human-rated spacecraft, specialized GN&C training and simulation is required for both for the crew and the ground operations team. Specialized GN&C training is required only for the ground operations team on robotic spacecraft missions.
8. Attitude control, line-of-sight pointing, and jitter (pointing stability) control performance is not a primary design driver on crewed spacecraft as it is on many of NASA’s robotic science spacecraft. Stringent attitude control is not typically required on crewed spacecraft. It should be noted that potentially certain payloads on crewed spacecraft (e.g., an optical communications terminal) may in fact need their own forms of precision pointing/pointing stability. However, that would be more the exception than the norm.
9. Robotic spacecraft, especially Astro-physics and Earth remote sensing space observatories, often have stringent instrument line-of-sight pointing and pointing stability requirements which drive the need for in-depth high-fidelity jitter modeling and analyses. Understanding, managing, and mitigating spacecraft jitter (also often referred to as “micro-vibration”) is a highly multi-disciplinary task that not only engages the attitude controls engineers but also the systems engineering, structural dynamics, mechanisms, and payload (e.g., optics) teams as well. References 30–35 (in Section 2.1, Addtional Post-2007 References) provide experiences, guidelines, insights, rules of thumb, potential design options, lessons learned, and best practices on the specific GN&C engineering topic of managing space observatory

line-of-sight jitter. For example, an important jitter engineering lesson learned is that there is no substitute for early sensitivity analyses specially when coupled to a complete pointing/pointing stability error budget. A complete error budget is absolutely needed at the start of a project with challenging micro-vibration requirements. Likewise, it is paramount to identify, early in the design cycle, all possible sources of on-board disturbances that can cause jitter. An observatory system-level Dynamic Interaction Test (DIT) to characterize jitter is the best way to gain confidence in an End-to-End model and performance predictions.

10. Robotic spacecraft rarely have requirements for rendezvous and docking, which greatly eases the GN&C DDT&E burden. Conversely, most human-rated spacecraft are required to possess some level of rendezvous and docking capability. However, it should be noted that robotic spacecraft may have requirements imposed on their design to support rendezvous and proximity operations needed to accomplish in-flight servicing (e.g., refueling).
11. Designers of typical robotic spacecraft GN&C systems do not typically address the type of aerodynamic flight control design challenges posed by satisfying EDL requirements.
12. Designers of typical robotic spacecraft GN&C systems tend to focus primarily on satisfying requirements for attitude determination and control as well as navigational requirements. Only rarely must the robotic spacecraft GN&C system designer address requirements for spacecraft guidance functions. The exceptions to this general rule are the rare occurrences when robotic satellites have requirements for rendezvous and docking.
13. Robotic spacecraft do not typically require the same levels of highly robust and reliable fault-tolerant processing capabilities found on human-rated spacecraft to support GN&C system FSW execution.
14. Human-rated spacecraft are flown by pilots, whereas robotic spacecraft are not. Therefore, far more than their counterparts working on robotic spacecraft, the designers of GN&C systems for crewed spacecraft must recognize and address the issue of “mode awareness.” Fundamentally, and in the context of this GN&C discussion, the problem of mode awareness focuses on the crew’s ability (or lack of ability) to clearly understand what specific mode the spacecraft’s GN&C system is in at any given time. The international aviation community has recognized the occurrence of mode awareness problems on the flightdeck of modern aircraft for several years. Fatal aircraft accidents have been attributed to mode errors by aircraft pilots. Some avionics companies are developing new flight control system designs to reduce the likelihood of such mode errors and to improve the pilot’s understanding of aircraft modes. A 1996 FAA study of this mode awareness problem on “highly automated aircraft flight decks” revealed at least four main points that should be factored into the design of future crewed spacecraft GN&C systems: 1) pilots had difficulty understanding the control algorithms of each of the modes; 2) pilots had incomplete or wrong expectations of flight control system behavior; 3) situations unforeseen by the flight control system designer lead to unexpected mode behaviors; and 4) pilots had difficulty anticipating the next flight control system state. Clearly the astronaut crew on a spacecraft should nominally have a combination of information from the ground operations team and on-board GN&C information displays for situational awareness, allowing them to monitor transition through the various GN&C operational modes, including abort and safe haven modes.

Modern and sophisticated spacecraft digital flight control systems will have many modes of operation, and in some such systems it may be relatively easy for the crew to transition from one mode into another without knowing it. This is because sometimes the transition between GN&C modes is automatic and not manually commanded by the crew. Mode errors occur when the crew assumes the GN&C is in one mode, when in fact it is actually in another mode. Similar crew inputs, while operating in different GN&C modes, could produce a drastically different, and possibly unsafe or hazardous, spacecraft response. GN&C designers, together with human factors engineers, must include design features to enhance the crew's ability to quickly and easily determine the actual mode of GN&C operation.

With regard to GN&C mode awareness, a three-pronged approach is recommended to: 1) eliminate, or at least reduce, the probability of "automation surprises" where the GN&C system takes unexpected actions and/or fails to take expected actions; 2) protect against a crew member preparing a mode (e.g., the loading mode-specific data into the flight processor) but forgetting to engage it; and 3) reduce errors of omission in which the crew fails to detect undesired GN&C behavior and fails to identify a mode error as the cause of the anomalous performance. Clearly much of the solution here is to enhance the crew's situational awareness of unfolding GN&C events. This can be accomplished with a system design that eliminates multiple modes that perform essentially the same task, enhanced GN&C displays that provide graphical and audio cues indicating mode transitions, a simple mode control interface, procedural design, and realistic crew training in high-fidelity simulators to exercise mission scenarios that represent to most safety-critical situations. The two primary takeaway points here are that GN&C mode awareness has a direct impact on overall system safety and that mode awareness issues are almost exclusively a GN&C design challenge for crewed spacecraft.

15. While spacecraft GN&C technology trends (for both crewed and robotic missions) are clearly moving toward onboard highly automated or even fully autonomous flight control systems, the expectation is that crewed spacecraft will always have some form of on-board manual flight control option available to pilots. Even with today's extremely automated and autonomous spacecraft, there is a critical and relevant need to design manual flight control modes with satisfactory handling qualities for each operational function [refs. 19, 20]. Defining measurable and predictable spacecraft handling qualities has been a concern since the beginning of crewed spaceflight. A lack of sufficient understanding of spacecraft handling qualities can lead to increased crew training requirements, additional pilot in-flight mental workload, undesirable flight control system interactions, and an inability to perform the mission/task. Unsafe, high-risk vehicle operations can result from poor handling qualities. Spacecraft handling qualities apply to both nominal and emergency operations. Manual flight control capabilities, if designed with handling in mind, will serve to make a spacecraft fly more robustly in the face of equipment failures, such as attitude control thruster failures.

    The requirements for spacecraft handling qualities must be an integral element of the GN&C systems engineering process for a piloted spacecraft. Ideally, specific vehicle attributes, defined early in the design and development process, will make handling qualities as compatible as possible with human operations. The spacecraft GN&C team, along with other engineering disciplines, must balance analysis of automated flight control modes/tasks with in-depth examination and testing of allowable and appropriate pilot inputs, based on offline

pilot models and human-in-the-loop simulations. Provisions for understanding, accommodating, and verifying spacecraft handling qualities should be incorporated directly into a crewed spacecraft flight control system's design, not considered as an afterthought. This will be a challenge for the GN&C community of practice, because no established spacecraft handling qualities design standards exist. All this points to the critical need for GN&C engineers to have easy access to a set of requirements that will enable a new generation of piloted spacecraft to be designed specifically for compatibility with human operation. Reference 28 addresses this need by providing a proposed set of concise design requirements for crewed spacecraft, which should yield satisfactory handling qualities when the pilot is performing manual flight control.

16. As described above, on human-rated spacecraft, the goal is to provide a manual control capability for the crew wherever possible. This is typically accomplished for all modes of GN&C operation where feasible on crewed spacecraft. However, during parts of both the powered ascent and the EDL mission phases the time-constants of the system dynamics are so short, relative to human detection/reaction times, that on-board manual human intervention by the crew is precluded. Manual control of robotic spacecraft is only very rarely performed (due to the large phase lag introduced by the relatively long round-trip communication time delays) and then only under extreme circumstances.
17. Given their mission class, and their associated relative priority, some robotic missions are severely challenged to secure communications (telemetry, tracking and command) services during all mission critical phases including the launch and the early in-flight operational period when so many failures occur. In some cases, the flow of GN&C engineering telemetry data during launch and the first few orbits is limited and this can impact the ground team's ability to perform real-time performance assessments and diagnose anomalies. Designers of robotic spacecraft GN&C systems need to keep this reality in mind and build in sufficient GN&C autonomy for early orbit survival. Human space flight missions are, appropriately because of the crew on-board, given the highest priority for communications services and can be assured of receiving a continuous flow of GN&C telemetry data from launch to landing.

In summary, according to the historical record, even though they were not driven by challenging crew safety requirements the designers of robotic spacecraft GN&C systems have had to consider many of the same GN&C architectural technical issues and operational concepts as their counterparts in crewed spacecraft design field. These issues and concepts were considered, even though there are differences in contingency management policies and allowing for the fact that they are not exactly identical GN&C engineering problems.

The general finding here is that while there are some distinct differences between the requirements for human-rated and robotic spacecraft GN&C systems the fact remains that several GN&C engineering lessons learned and best practices emerge from the robotic spacecraft arena that should apply in an equally appropriate manner to the design and development of GN&C subsystems for crewed, human-rated spacecraft.

1.6 GN&C Best Practices

In this section, the comprehensive list of 22 GN&C best practices as identified by this NESC study process are provided. These best practices are divided into "Early Work" and "Late Work" categories, consistent with the overall philosophy of this report.

The Early Work best practices will properly guide GN&C designers through the complex and iterative process of converting top-level requirements and operational concepts into a GN&C subsystem architecture that is feasible, affordable, reliable, and implementable. These particular best practices have been found to promote and enforce the necessary high-level abstract thinking and design consideration work needed early in the DDT&E process to ensure the "right" GN&C system is conceived for a given spaceflight mission. The Early Work steps of the GN&C DDT&E process are depicted in Figure 1.6-1 for reference.

The Late Work best practices will properly guide GN&C engineers through the process of translating the designers' architectural intent into a physically real space flight system. These practices have been found to both avoid workmanship problems, and to trap flaws in the design, build, integration, test and operation of the spacecraft GN&C subsystems. The Late Work steps of the GN&C DDT&E process are depicted in Figure 1.6-2 for reference.

It should be noted that many of the Early Work best practices apply to, and would normally be extended into, the Late Work phase of the DDT&E process. For example, the analysis of the spacecraft dynamics in all flight phases (i.e., #13) will certainly be initiated early on in the GN&C development cycle, but will just as certainly continue right up through launch and beyond.

Many sources were used while gathering and uncovering relevant information for this section. The team performed an all-source "search and capture" process from which emerged a set of common recurring GN&C lessons learned and associated best practices. These common GN&C "mission success" themes and elements were seen across crewed and robotic spacecraft lines, as well as across NASA and DoD spacecraft lines and across industry and government organizational lines as well. The sources included:

- NASA MIB Reports
- Technical documents, reports, articles, and conference papers
- NASA Lessons Learned Database
- GSFC Rules for the Design, Development, Verification, and Operation of Flight Systems—GOLD Rules[5]
- Aerospace Corporation's Space Systems Engineering Handbook (Chapter 10) and "100 Review Questions to Ask" document
- Interviews with senior GN&C engineers inside and outside NASA

Several of the above sources have been summarized in this document's appendices to provide ready-to-hand references. Each best practice is mapped to one or more items from the appendices

[5] The Goddard Open Learning Design (GOLD) Rules specify sound engineering principles and practices, which have evolved in the Goddard community over its long and successful flight history. They are intended to describe foundational principles that "work," without being overly prescriptive of an implementation "philosophy."

to provide a direct linkage for the reader to concrete lessons learned from "real world" examples of space system GN&C mishaps and/or failures. The GN&C relevant appendices are:

Appendix A Selected GN&C-Related Robotic Spacecraft Mishaps/Failures

Appendix B GN&C-Related Lessons Learned Extracted from the NASA Lessons Learned Information System (LLIS)

Appendix C GN&C-Related Best Practices Extracted from the NASA GSFC "GOLD Rules" Database

Appendix D GN&C-Related Lessons Learned Extracted from the Aerospace Corporation Document, "100 Questions for Technical Review"

Appendix E Gimbaled vs, Strapdown Inertial Systems

Appendix F Apollo Guidance, Navigation, & Control System Components

Appendix F Use of Bond Number to Determine Liquid Slosh Regime

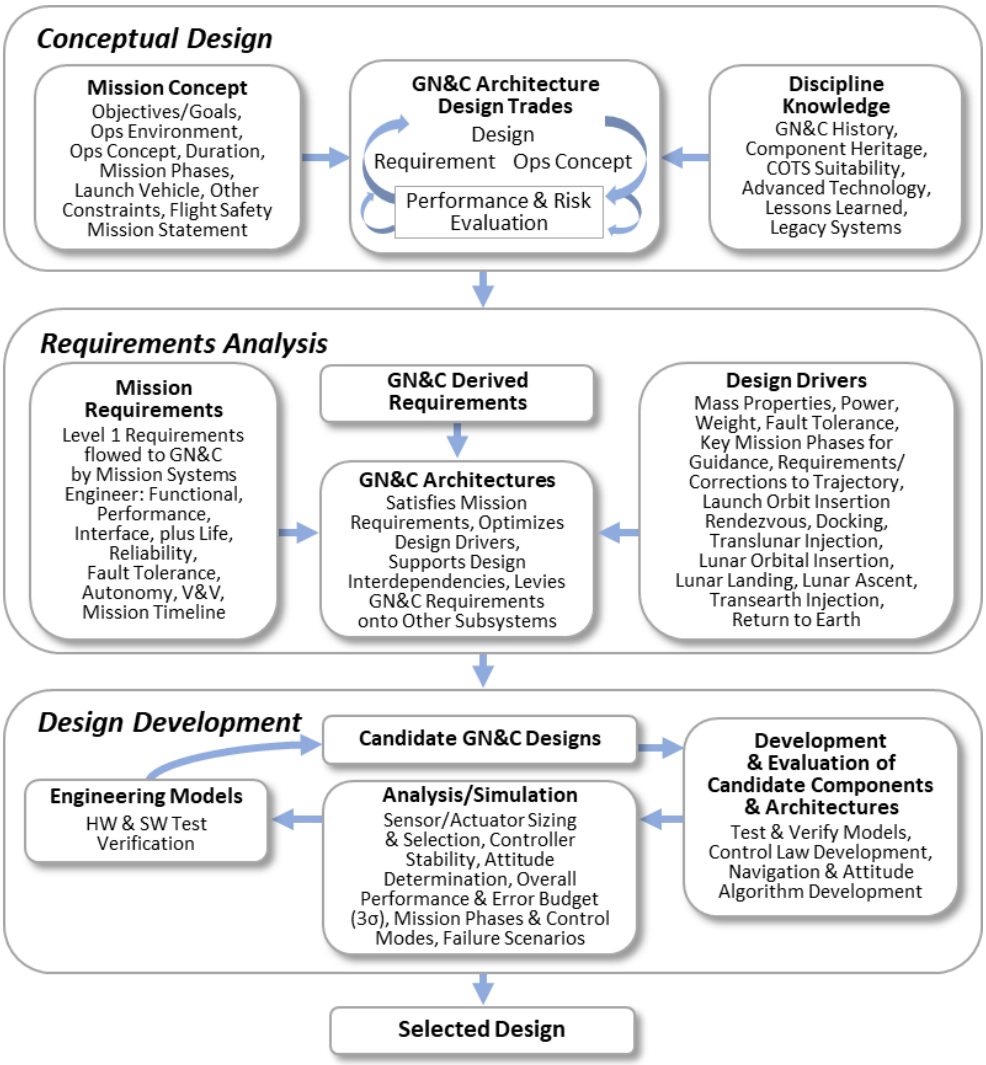


Figure 1.6-1. GN&C Design & Development Process – Early Work

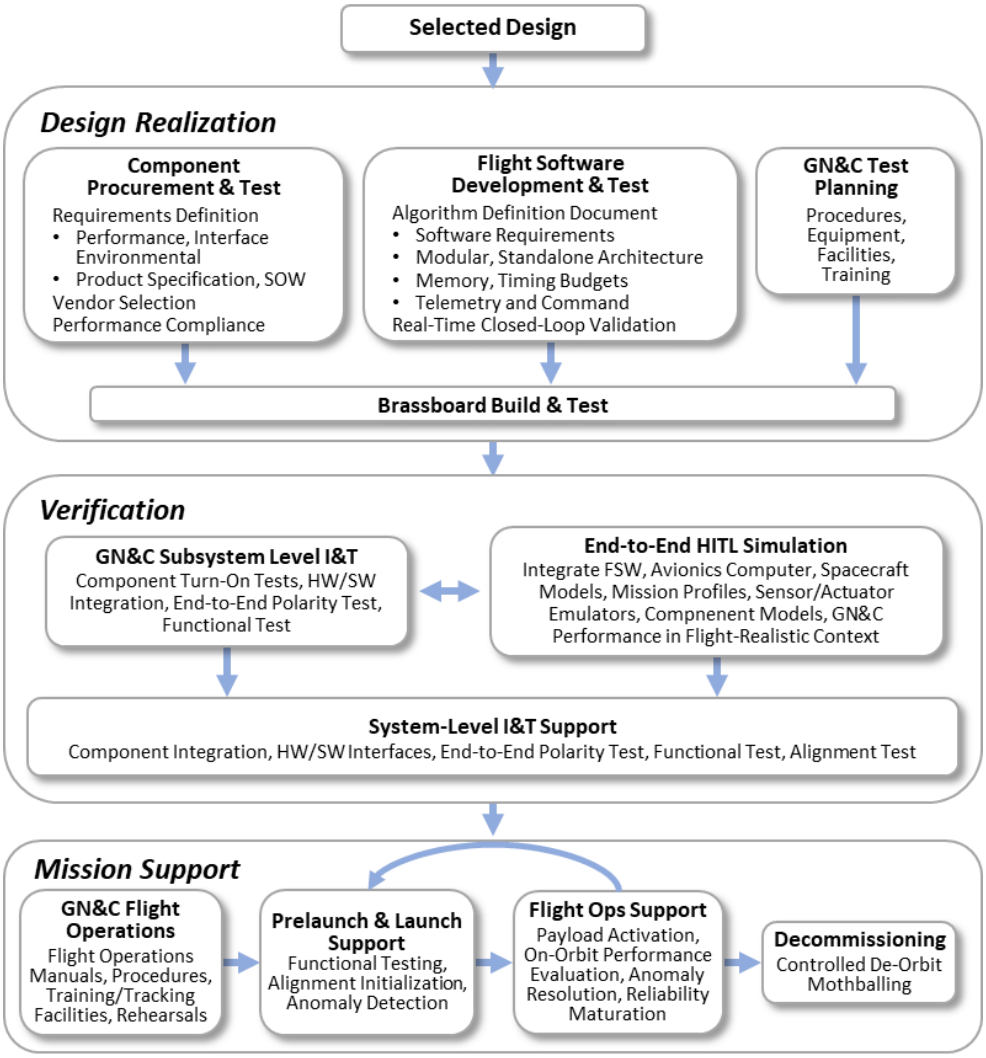


Figure 1.6-2. GN&C Design Process – Late Work

Early Work Best Practices

Early work best practices enable designers to capture the breadth and depth of design drivers, which is necessary for accurate evaluation of candidate designs.

1. Conduct a comprehensive and iterative GN&C subsystem architectural development activity early in the DDT&E process.
2. Search out, identify, and define all the interdisciplinary interactions and relationships that exist between the GN&C subsystem and other spacecraft subsystems.
3. Ensure that a comprehensive abort/safe haven strategy has been formulated, and that abort and/or safe haven functional capabilities are implemented, for all mission phases.
4. Host mission-critical GN&C FSW processing functions on a spacecraft processor with sufficient computational power and assign sufficient processing priority to execute at the necessary frequency established by analysis.

5. Ensure that autonomous GN&C fault management is independent of all hardware and software that might be involved in either causing or diagnosing a fault.
6. Establish and flow down the higher level of GN&C requirements necessary for a multi-vehicle system of spacecraft that must safely interact during the rendezvous, proximity operations, docking/undocking, and/or mated operational mission phases.
7. Critically evaluate redundancy with identical GN&C hardware components to ensure that the net effect is an overall increase, rather than a decrease, in system reliability. Always keep in mind that redundancy inherently adds complexity.
8. Evaluate all heritage hardware and software elements in the GN&C architecture in light of potential differences in build, flight configuration, mission application, flight operating environment, and design/operations teams.
9. Make certain that new GN&C technology is well qualified. It must have sufficient statistics to show an acceptable safety margin, and flight-proven alternatives must be identified.
10. Design for Test: Consider the degree of difficulty of performing ground validation testing and pre-flight calibration when evaluating candidate GN&C subsystem architectures.
11. Define and document the coordinate frames and the system of units (and associated conversion factors) that are to be employed, and rigorously enforce compliance.
12. Ensure controller designs meet or exceed the following gain and phase margin stability criteria as a function of GN&C design maturity.

State of Design Maturity	Gain Margin	Phase Margin
Continuous analysis during preliminary design	12 dB	45°
Critical Design Review (CDR)-level sampled data analysis with actual FSW digital implementations and final flexible body models	6 dB	30°

13. Ensure the analyses of the dynamics in ALL flight phases are understood completely (e.g., aerodynamics, structural flexibility, damping, gyrodynamics, plume impingement, moving mechanical assemblies, fluid motion (i.e., propellant slosh), changes in mass properties, thermal snap).
14. Make certain that the analyst who develops the mathematical models for the simulation of the GN&C hardware has hands-on familiarity with the hardware being modeled. All unexpected results or anomalies during hardware testing must be explained and/or incorporated into the simulation math model. Similarly, all deviations between results from the design simulation and the V&V simulation must be explained. Re-used heritage models from similar missions, along with their intrinsic assumptions, must justify their application through testing in the relevant new environments
15. The truth model used in verification of high-fidelity simulations must be developed independently from that used in the design simulation.

Late Work Best Practices

Late work best practices enable engineers to translate the designers' intent into reality. These practices have been found to both avoid workmanship problems, and to trap flaws in the design, build, and integration of the subsystem.

16. Establish a strong relationship with, and maintain close surveillance of, the GN&C lower-tier component-level (both hardware and software) suppliers.
17. Ensure the GN&C subsystem adheres to the "Test As You Fly" philosophy. Create a Test As You Fly Exception List documenting specifically where this test philosphy is not adhered to, including a description of the accepted risk to mission success.
18. Plan and conduct true end-to-end sensors-to-actuators polarity tests in all flight hardware/software configurations, including all flight harnesses/data paths, consistent with the "Test As You Fly" philosophy. Resolve all test anomalies.
19. Plan and conduct sufficient GN&C hardware-in-the-loop (HITL) testing to verify proper and expected hardware and software interactions in all operational modes, during mode transitions, and in all mission-critical events.
20. Treat GN&C ground databases, uploads, ground application tools, command scripts/files, etc. with the same disciplined care used for the GN&C FSW code and data.
21. Ensure that sufficient GN&C engineering telemetry data are down-linked to diagnose anomalies, particularly during all mission-critical phases, including the early on-orbit operational period when so many failures occur.
22. "Train as They Fly"—Ensure that a dedicated real-time GN&C simulator facility is developed and maintained to allow the crew to realistically train and rehearse GN&C operations in the manner that they expect to actually fly the spacecraft.

GN&C Best Practice #1

Conduct a comprehensive and iterative GN&C subsystem architectural development activity early in the DDT&E process.

Discussion:

The up-front "architecting-in" of robustness and reliability must be an integral part of the early steps of the GN&C systems engineering process. Inferior architectures may be overly complex, difficult to produce, test, operate, support, service, upgrade, and are often prohibitively costly to adapt to evolving mission scenarios as the life-cycle extends beyond the anticipated time frame of the spacecraft's service life. An inferior GN&C architecture can also be "brittle" with few robustness qualities. Desirable GN&C architectures allow for growth in the mission set and have high measures of effectiveness, safety, reliability, affordability, and sustainability.

GN&C systems for future crewed space platforms will likely be embedded in both space and ground assets. Exactly how the GN&C architecture allocates functionality across both space and ground assets can have long-term impacts on the effectiveness and cost of operations over the life-cycle. Careful consideration must be given to the integration of hardware and software. A minimum set of sensor/actuator hardware that can be flexibly re-configured with minimum human interaction would be highly attractive. GN&C software consisting of standardized and modular algorithms applicable to a broad range of exploration vehicles and missions would also be of great value. Common fault-tolerant computational architectures would improve reliability and reduce development costs. These hardware and software attributes would presumably have high spacecraft life-cycle value by supporting robust, reliable, and responsive exploration mission operations.

Clearly, the selected architecture will directly influence the physical complexity, functional behavior, and performance of the GN&C subsystem, along with the related properties of safety, ease of implementation, operational complexity, affordability, robustness, serviceability, adaptability, flexibility, and scalability. A superior architecture for most spacecraft GN&C subsystems typically emerges from multiple iterations between the architects/designers and the stakeholder/customer/end user communities. Architectural design is therefore an iterative loop, where the expected reliability of necessary components dictate the level of functional and hardware redundancy.

The migration of the Apollo Block I GN&C architecture into the Apollo Block II GN&C architecture is an excellent and concrete example of how the GN&C for a human rated spacecraft will naturally evolve over the early phases of the program. The two basic Apollo GN&C system configurations were referred to as Block I and Block II. The Block I system was designed when the Command and Service Modules were to be landed on the moon. To achieve the system reliability required by this plan, spare units were to be carried on board, and in-flight maintenance was to be performed. However, inherent problems existed in this concept that were never really solved, such as moisture getting into electrical connectors during change-out. The adoption of the Lunar Orbit Rendezvous (LOR) strategy advocated by Houbolt was the principal driver for the implementing the Block II GN&C changes [ref. 28]. That decision point provided a logical time to change to the Block II configuration that, because of redundant paths, negated the in-flight maintenance requirement and thereby avoided the connector problem. The Block II

system was smaller, lighter, and more reliable than the Block I design. Another advantage was that the primary guidance systems for the CM and the LM could be nearly alike.

When looking back from today's vantage point, it is quite easy to see that the June 1962 decision to commit to the LOR approach was arguably one of the most fundamentally important management decisions made during the Apollo Program. What is remarkable, and what is important for today's generation of NASA architectural planners to note, is that this very important LOR decision was made relatively early in the Apollo Program. In fact, it was made at a point where less than 1% of the total $19 billion Apollo budget had been spent [ref. 29].

An article from 1964 [ref. 31] provides another viewpoint on how the Block I Apollo GN&C concepts underwent a number of evolutionary changes intended to improve mission flexibility and reliability and save weight and space in the spacecraft. In the Block I design, the inertial Guidance/Navigation subsystem being developed by MIT-IL fed its output signals through the Honeywell-developed Stabilization/Control subsystem to operate the service module propulsion engine and reaction control thrusters. With the two subsystems connected in this "series" configuration, a failure in the Honeywell subsystem could incapacitate the Guidance/Navigation subsystem. In the Block II configuration, the previous series configuration was changed to better integrate the two subsystems while making them electrically independent. The obvious benefit being that a failure in one does not affect the other. This was achieved by increasing the capability of the Guidance/Navigation computer so it could handle the Stabilization/Control tasks, thereby becoming the primary portion of the integrated guidance, navigation and control system [ref. 31].

Another two items that bear on GN&C architectural development come directly from the Shuttle Orbiter Flight Control System (FCS) design lessons learned [ref. 26]. As cited, the late recognition of GN&C hardware constraints required an extensive "late" effort to develop FSW revisions and to re-verify this modified software. This lesson learned from Shuttle points out the benefit of having a GN&C architecture that provides software flexibility and reconfigurable design constants that can reduce the impact of late emerging hardware constraints. Another Shuttle Orbit FCS lesson learned, also identified in reference 26, had to do with the consequences of "late" recognition of the FSW design impacts and operational procedure complexities of incorporating automatic GN&C failure reconfiguration functionality in the GN&C architecture.

Interviews with Apollo-era GN&C developers emphasized that early "hands-on" involvement by astronauts/crew in the formulation of the GN&C architecture is a must. Early involvement and participation by system operators in GN&C system architectural decisions, and the subsequent design iterations, should return a significant payoff in safe and reliable mission operations over the spacecraft lifecycle.

Lastly, it is important to stress the need for and the use of error budgets to help guide the formulation of GN&C design concepts early in the DDT&E process. The creation of error budgets is a fundamental task in the GN&C analysis process. Typically, error budgets are constructed for the navigation, pointing knowledge, attitude control, and stability of a spacecraft. Separate and distinct error budgets will need to be developed for each mode of GN&C operation. Therefore, it is not uncommon for a single mission to have multiple error budgets. Error budgets are made up of multiple individual line item allocations. These error budgets are used to

systematically decompose, partition, group, and allocate performance requirements across the elements of a GN&C system. Preliminary error budgets are typically constructed based upon initial best estimate assumptions of the quantitative performance (as demonstrated on past similar missions) of navigation sensors, navigation algorithms, targeting algorithms, attitude determination sensors, attitude/flight control algorithms, the clock/timing subsystem, attitude control actuators, and other GN&C functional elements.

The individual line-item error sources are then summed together in a statistically appropriate manner to determine if the overall estimated GN&C system-level performance can satisfy the GN&C performance requirements for that particular mode of operation. The error budget will also reveal the margin between the predicted performance and the required performance. The error budget also serves to identify the predominant source(s) of GN&C error for a given mode and to point out the "tall pole" error source(s) as specific areas for the GN&C system designer to focus attention on. The GN&C designer can use error budgets as a "what if" tool to parametrically explore sensitivities in system performance to variations in selected error sources.

Error budgets can be used to define specifications/constraints on navigation sensor performance, attitude determination sensor performance, algorithm accuracy, attitude control actuator performance, clock/time reference accuracy, structural misalignments, thermal distortions, etc. Preliminary error budgets constructed early in the DDT&E process must be successively refined and updated to reflect the changing GN&C system design and any changes to GN&C requirements. The verification of each error budget line item allocation will need to be performed either via analysis, modeling and simulation, demonstration, inspection and/or test. The system of units used in an error budget should be consistent for all line items. It should also be clearly noted if the values used in the budget are either 1-sigma, 3-sigma or worst case allocation numbers.

Mission and/or Lesson Learned Linkages:

References 26, 28, 29, and 31

Relevant Questions:

1. Have all the high-level mission, system, and subsystem functional, performance, and interface requirements that typically drive the nature of the GN&C architecture been defined and documented? Have these requirements been clearly communicated to the architectural definition team?
2. Have all the unique GN&C subsystem operational states/modes to be employed throughout the mission life been identified? What are all these states/modes? What specifically distinguishes these states/modes from each other? Where is there commonality between states/modes? Have all state/mode transitions been identified?
3. For each GN&C mode, have the mission phases where this mode is utilized and the bounding requirements on environment, vehicle dynamics, and performance and reliability/fault tolerance been determined?
4. Have preliminary GN&C Error Budgets been formulated for each GN&C mode of operation? Do these budgets take into account the specific sensors, algorithms, and actuators envisioned to be used in each mode? Do these error budgets allocate performance levels to each element of GN&C hardware and software (algorithm) such that the desired performance requirements

are met? What is the basis-of-estimate for, and source of, the numerical entries on each line of each error budget? Are all of the entries expressed in the same number of standard deviations (e.g., 1-sigma, 3-sigma) or maximum NTE values? What is the rationale for the method used to combine the different contributors into a total error allocation? How will performance against the budgeted allocation(s) eventually be verified?

5. Have multiple candidate GN&C architectures been defined and developed? Have all architectural trade studies been identifed and conducted? What process, criteria, and measures of effectiveness were used to assess and evaluate these competing GN&C architectures?
6. What is the conceptual basis and technical rationale for the overall GN&C architecture selected? Which particular GN&C requirements drove the selection of this architecture?
7. Has the GN&C architectural definition team carefully considered the use of the algorithms, software, and actuator/sensor types previously flown on missions with similar objectives and performance/reliability requirements?
8. What process was used to select the type, size and number of the GN&C sensor and actuator hardware components? Similarly, how were the GN&C algorithms and flight/ground software elements selected?
9. Was the selection of the GN&C navigation and attitude sensor suite based upon performance requirements as well as the need for diversity of sensors in order to provide the capability to identify and eliminate faulty sensors?
10. Have any and all single-point failures in the selected GN&C architecture been identified and documented? Is there an established process for the comprehensive consideration of the single-point failures? If so, does this process require an examination of risk mitigation approaches and does it provide a risk acceptance rationale?
11. Has an assessment been performed of how well the GN&C candidate flight hardware can perform/operate/survive in the prescribed envelope of planned spacecraft flight environments (thermal, vibration, radiation) and operational regime (rates, acceleration, precision / accuracy)?
12. During the GN&C architectural development process, what considerations have been given to the degree of difficulty in GN&C subsystem hardware/software integration, testing, and flight operations?
13. How will the crew interact with the GN&C? What kind of hand controls and displays will they need? If need be, will the GN&C architecture allow the spacecraft to be “pilotable” by a single crewmember?
14. Does the GN&C architecture employ sensors and actuator hardware common to other space based elements of the overall Exploration architecture?
15. How does the selected GN&C architecture accommodate the requirements for multi-vehicle interaction? How is it envisioned that the spacecraft’s GN&C will interact/interface with the GN&C subsystems of other spacecraft when mated? Does the spacecraft GN&C architecture include provisions for command/telemetry/data interfaces to allow the use of GN&C sensors and actuators on other vehicles during mated operations?

16. If the GN&C architecture is to employ a diverse set of sensor/actuator components, in order to provide functional redundancy, has an estimate been made of the total resources that will be needed to source/procure, qualify, test and integrate all these components?
17. Does the GN&C architecture permit navigation strategies that rely on diverse inputs including those from inertial sensors, optical sensors, the crew and the ground?
18. Does the selected GN&C architecture recognize and compensate for the fact that GN&C sensor/actuator components are subject not only to failure and malfunction, but also degradation over the mission life? What assumptions have been made regarding sensor/actuator degradation? How have these degradation assumptions affected the design and capability of the FDIR elements of the GN&C architecture? How have these degradation assumptions affected contingency planning?
19. Has an abort/safe haven strategy been formulated that is compatible with the selected GN&C architecture? What provisions in the selected architecture provide a GN&C backup capability that keeps the crew "safe" should the primary systems fail or become temporarily unavailable? What are the abort modes, and how does the GN&C architecture support their operation? Does the selected GN&C architecture provide a safe haven attitude control mode capability?
20. Does the selected GN&C architecture provide the crew with a completely independent implementation of all critical GN&C functions? If so, can these independent GN&C functions be enabled manually if necessary?
21. To what extent has the crew had involvement in the architectural definition of the human-rated spacecraft's GN&C system, especially in the area of the GN&C/Human interactions such as displays and hand controllers?
22. How sensitive/vulnerable is the GN&C architecture to faults, degradations, and failures in other spacecraft subsystems to which it is coupled and reliant upon?
23. How will the GN&C sensors and actuators be physically accommodated in the spacecraft? Do all GN&C RF/optical navigation sensors have suitable unblocked fields of view? Are there requirements to co-locate certain GN&C components (e.g., inertial sensors and optical sensors)?
24. Is in-flight servicing to be performed? Which specific GN&C components should be serviceable? Are there physical accessibility requirements in order for the crew to perform on-orbit servicing of GN&C components from inside the spacecraft (e.g., swap-out of an IMU)?
25. How reconfigurable will the system be? Will the crew have the operational flexibility to "mix and match" the available GN&C sensors and actuators?
26. What provisions are included in the GN&C architecture for upgradeability? Are simple, standard interfaces employed to directly support, and make practical, upgradeability? Keep in mind that subsystem modularity alone is a necessary condition for upgradeability but is not a sufficient condition.

GN&C Best Practice #2

Search out, identify, and define all the interdisciplinary interactions and relationships that exist between the GN&C subsystem and other spacecraft subsystems.

Discussion:

An extremely important role of the GN&C System Engineer is the communication and coordination with other spacecraft subsystem leads. Experience has shown that neglecting, ignoring, over-simplifying, or overlooking the critical need for compatible design interactions between the GN&C subsystem and the other spacecraft subsystems can lead to mission mishaps and/or failures. The GN&C SE needs to fully understand and appreciate the GN&C subsystem's relationship and interactions (in all forms) with the other spacecraft subsystems. All such relationships and interactions should be rigorously documented. Specific cases where the lack of full understanding and proper treatment of these relationships has led to failure or mishap include the TIMED and DART missions. See Tables 1.4-1 and 1.4-2 in Section 1.4 for common interactions between GN&C and other subsystems.

Uncertainties and ambiguities in the interfaces between payload subsystems and the spacecraft GN&C subsystem, on some robotic spacecraft, have not compromised the reliability of the GN&C, but have compromised the ability of the observatory to actually meet the desired pointing requirements.

The GN&C subsystem lead needs to fully define, through negotiations with other subsystem leads, and formally document the following:

1. A summary description/schedule of those products that the GN&C subsystem lead needs to deliver to either the other spacecraft subsystem leads for their use in their subsystem-level design process or to the spacecraft systems engineering lead. Those products may include GN&C trade study results, requirements documents, interface control documents (ICD)s, error budgets, data/signal flow charts and block diagrams, work plans and schedules, technical memos, reliability analyses, fault trees, failure modes and effects analyses, test procedures, test reports, analytical procedures, analytical model interface requirements, analytical models, testbed and/or lab requirements, test article requirements, algorithm definitions, software builds, electrical harness diagrams, etc.
2. A summary description/schedule of those products/documents the GN&C subsystem lead expects to receive from either the other subsystem leads or from the spacecraft systems engineering lead to be used in the GN&C design process.
3. Mission and/or Lesson Learned Linkages:
   Appendix A: TIMED, DART

Relevant Questions:

1. Have all the interfaces and interactions between the GN&C subsystem and all the other spacecraft subsystems been clearly defined and documented? For example, has it been determined whether the GN&C subsystem will be responsible for controlling steerable/pointable spacecraft appendages such as communications antennas and solar arrays?
2. Have all the uncertainties and ambiguities, as well as the specific hardware/software faults, degradations, and failures, in other spacecraft subsystems that will affect the GN&C subsystem been identified? Has the potential impact of these been factored into the overall GN&C risk posture?
3. Have lists of GN&C products/documents, both deliverables and receivables, been generated? How were they developed? What technical interaction occurred to formulate these lists? How does one know the lists are comprehensive?
4. Are there formalized "agreements" or "commitments" in place between the individual subsystem leads (and between the subsystem leads and the systems engineering lead) to ensure the required products deliveries occur on time/within budget in both directions?
5. Have all the listed GN&C product deliveries been costed and budgeted by the project?
6. Has the entire necessary infrastructure (i.e., computer-based tools, engineering test unit hardware, testbeds, dynamic models, etc) been identified and costed and budgeted to support the generation and delivery of all the listed GN&C products?
7. Has an integrated schedule of all subsystem product deliverables and receivables been developed? If so, has a product delivery critical path analysis been performed? Is the relative phasing of products acceptable? For example, will the necessary detailed mass properties information be delivered to the GN&C team in time to allow for sufficient stability and controllability performance analysis? Are any GN&C subsystem product deliverables and receivables on the critical path? What steps have been taken to eliminate/mitigate schedule conflicts for the GN&C team?

GN&C Best Practice #3

Ensure that a comprehensive abort/safe haven strategy has been formulated, and that abort and/or safe haven functional capabilities are implemented, for all mission phases.

Discussion:

The fundamental difference between the GN&C design of crewed spacecraft and that for robotic spacecraft is that the presence of humans on-board necessitates the means to be able to safely return them to Earth. Safety of the crew is of paramount importance.

The GN&C system is designed to operate under routine (nominal plus reasonable uncertainty factors) flight conditions. However, the GN&C system design and capabilities must also function to ensure the safety of the crew under the extreme flight conditions when severe spacecraft (and launch vehicle) system degradations, malfunctions and failures occur.

Robotic spacecraft GN&C designs do not typically have abort modes of operation. A GN&C system for a robotic spacecraft however will typically include one or more safe haven modes that provide a power-positive, thermally safe, form of backup attitude control to be entered in the event of a spacecraft emergencies. A safe haven mode implementation should be as simple as practical, employing the minimum hardware set required to maintain a safe spacecraft attitude.

To be more specific a safe haven mode (also often referred to as a "safe hold mode," or SHM) is a temporary state of minimized spacecraft operations that is transitioned into as a result of an autonomously irreconcilable spacecraft fault or failure. While in this safe haven mode all mission payload operations are suspended and, if necessary, instrument/sensor optical protections are enabled. The vehicle is configured for sufficient solar array power collection to support minimal spacecraft power consumption which is accomplished through load shedding steps. Adequate thermal control is also performed to ensure spacecraft components remain in a healthy state. In addition a spacecraft command and telemetry communications link is maintained to support the resolution of the spacecraft fault or failure. This communications path might very well be a low data rate link but it should be sufficient to re-establish normal spacecraft and payload operations. Prior to launch, a decision should be made as to whether or not to test the safe haven mode(s) in-flight. A rigorous risk/benefit assessment should be performed to support that decision regarding the in-flight safe haven test.

Crewed spacecraft would likely benefit from having safe haven modes of operation in addition to a comprehensive set of abort mode capabilities. For example, it would be prudent to have a safe haven attitude control mode in place for those periods of the flight where the crew is not providing continuous watch. This safe haven capability might be particularly useful on missions to the Moon, and certainly to Mars, where there will be a long-endurance cruise phase.

An abort strategy must be formulated to drive the actions to be taken to remove the spacecraft (with its crew) from an intolerably un-safe and possibly hazardous dynamic state. This un-safe condition could arise from many different problems that span the entire mission envelope. A launch vehicle propulsion system problem will, after the extension of all possible pre-Abort options, trigger an abort. Likewise, during rendezvous operations, the determination that the chaser spacecraft is on a collision course with the target spacecraft should also trigger an abort.

Aborts during launch and ascent will prematurely terminate the mission in order to return the crew safely to Earth. There could possibly be abort scenarios where the mission is continued but with highly altered and much less ambitious objectives than were originally planned. In other cases, an abort could result in the spacecraft being temporarily placed in a safe haven mode. For example, an abort during the terminal phases of a rendezvous could trigger an orbital maneuver to enter a safe collision-free orbit and then place the spacecraft in a safe state.

Safe haven modes independently and reliably place the spacecraft in a safe state to allow the crew (and ground if a communications link is open) a reasonable amount time to diagnose and troubleshoot in-flight problems.

Abort planning, and the definition of specific abort modes, is a daunting and complex systems engineering responsibility. The development of an effective, affordable, and implementable abort strategy is especially complex because of the myriad of potential mission contingencies that should be identified and evaluated [ref. 32]. The abort strategy will be heavily influenced by the spacecraft GN&C architecture, design features and performance capabilities. Conversely, as the requirements for certain abort capabilities are refined they may drive changes to existing GN&C architectures, design features, and capabilities. The actual implementation of abort mode functionality will most likely be accomplished with a combination of flight hardware subsystems/components and on-board autonomous software.

Abort planning will first consider those phases of the mission where risk levels are the highest. For NASA human rated crewed spacecraft, these high-risk phases occur at the beginning and the end of each mission. That is to say they occur during the launch event itself (booster ignition), during the powered flight ascent trajectory into the mission initial orbit about Earth, and during the EDL phase of the mission. These are also the phases of the mission where the time-constants of the system dynamics are so short (relative to human detection/reaction times) that extensive on-board human intervention by the crew is precluded. This is the principle driver for employing on-board autonomous “abort manager” software to rapidly detect an anomalous condition during launch, ascent and/or the EDL phases and take steps to either resolve the anomaly (e.g., by swapping out a “bad IMU for a “good” IMU) or to trigger the initialization of a pre-planned abort mode.

The crew should nominally have a combination of information from the ground operations team and on-board GN&C information displays for situational awareness allowing them to monitor transition through various pre-defined abort regimes and, if necessary to supervise an unfolding abort condition.

For example, on the Shuttle, the flight crew selects the abort mode by positioning an abort mode switch in the cockpit and depressing an abort push button. The Shuttle Mission Control Center (MCC) is prime for calling for any abort because it has a more precise knowledge of the Orbiter’s position and velocity than the crew can obtain from onboard systems. Before Main Engine CutOff, the MCC makes periodic calls to the crew to tell them which abort mode is (or is not) available to them. If during ascent communications with the MCC are lost, the flight crew has onboard methods, such as cue cards, dedicated displays, and display information, to determine the current abort region. Note that as part of the Shuttle Cockpit Avionics Upgrade effort, new algorithms and displays were developed for the Shuttle Abort Flight Management application.

Abort planning should cover a wide range of potential system degradation, malfunctions, and failures. Anomalous conditions such as launch vehicle engine failures, engine under-performance, propellant tank leakage, crew cabin pressure leakage, loss of electrical power, loss of vehicle cooling, etc. are typically considered when doing abort planning. A detailed risk assessment analysis should be used to guide this abort planning work. The number, type, and order of abort modes will be driven by several factors, such as:

- The type of failure.
- The failure probability of occurrence.
- The impact to system operation/performance if the failure does occur.
- The time range over which the failure can occur (along with the understanding of specifically when in that range it is most likely to occur).

The abort planning process should also clearly define the order of preference for the various abort modes. In cases where performance loss is the only factor, the abort mode chosen is the highest one that can be completed with the remaining vehicle performance capability. The abort mode selected depends on the cause and timing of the failure(s) and which abort mode is likely to be the safest.

Good spacecraft engineering practice would dictate the consideration of a safe haven attitude control mode to be entered in spacecraft emergencies. A safe haven attitude control mode is independent of the spacecraft's primary mode of attitude control. Its primary purpose is to rate stabilize the spacecraft by damping angular velocities rates to within pre-set limits. Secondary purposes are to stabilize the attitude of the spacecraft in a power-safe and thermal-safe orientation that allows communications with the ground operations to be re-established.

It is mandatory that the safe haven mode should behave very predictably while minimizing its demands on the rest of the spacecraft. This facilitates the survival, diagnosis, and recovery of the larger spacecraft system. The GN&C equipment used to implement this safe haven function should be separate from the equipment used by the primary spacecraft attitude control system. The safe haven mode equipment could be entirely independent from the primary mode equipment or may be the redundant side of a dual-redundant primary component. The safe haven attitude controller (i.e., the control law logic) may be either hosted on a dedicated standalone, possibly dissimilar, safe haven processor or hosted in a redundant primary flight computer.

The safe haven mode design must take into account the spacecraft thermal design, structural design including array orientation and mass properties, and attitude control electronics design. The safe haven is driven by the GN&C subsystem, but clearly is a spacecraft system-level issue.

Mission and/or Lesson Learned Linkages:

- Appendix A: Lewis
- Aerospace LL #35, 36
- GSFC GOLD Rule #1.17
- Reference 32

Relevant Questions:

1. What are the abort strategies for the various phases of the mission such as ascent, LEO cruise, trans-lunar injection, lunar cruise, lunar orbit injection, lunar landing, lunar rendezvous, and entry?

2. Does the GN&C subsystem design include provisions for a safe haven attitude control mode that will autonomously (i.e., based upon pre-defined dynamic conditions and without ground interaction) activate upon the diagnosis of a spacecraft emergency?
3. Do both the GN&C requirements document and the mission concept of operations documents include detailed information concerning abort scenarios and the safe haven modes?
4. Can the safe haven mode be manually commanded by the crew if necessary?
5. Is the safe haven mode implementation as simple as practical, employing the minimum hardware set required to maintain a safe spacecraft attitude?
6. How will the GN&C recover from a loss of control/lost in space condition? Will the recovery require support from the ground or will the GN&C recover in a completely on-board cold-start manner? If on-orbit, will it be completely automatic or will the crew need to take action?
7. What is the operational concept for "powering on" from a cold start condition and initializing the GN&C subsystem? Is it a deterministic procedure/process or not? How long does it take to power on, initialize and bring "online" the GN&C subsystem? Likewise what is the operational concept for placing the GN&C subsystem into a standby (power saving) mode? How long does it take to bring the GN&C back online from standby mode?
8. Has the GN&C hardware & software configuration for safe haven mode been identified?
9. Are passive abort schemes employed wherever feasible, especially during rendezvous?
10. What attitude control electronics (processor and bus) are available for safe haven control algorithm implementation? How independent are these attitude control electronics from the primary mode equipment?
11. What sensors will be used for the safe haven mode?
12. Has a detailed safe haven mode design been established including entry/exit criteria and the associated fault management requirements on FSW?
13. Subsequent to its activation, will the safe haven mode require crew and/or ground intervention for continued safe operation? How long can the spacecraft operate in the safe haven mode without the need for crew or ground interaction? What are the constraints driving the need for such interaction by the crew or ground?
14. Has the contractor demonstrated, via a FMEA approach or similar type analysis, that no single credible fault can both trigger safe haven entry and cause safe haven failure?
15. For safe haven, can passive stability (via a slow spin about the maximum moment of inertia axis or via gravity gradient) be used to stabilize the spacecraft in a thermal and power safe mode?
16. What safe haven attitudes are acceptable for thermal, power, and communications safety?
17. Has the performance of safe haven attitude controller (control law logic) been analyzed and verified in the HITL test environment?
18. Have proper safe haven mode transitions been verified in HITL testing?

19. Have safe haven recovery procedures been developed and validated during mission simulations?
20. Will the safe haven mode be tested on-orbit? Has a rigorous risk assessment been performed to support a Project-level decision as to whether or not to perform an on-orbit safe haven test? What is the rationale for (or against) an on-orbit safe haven test?

GN&C Best Practice #4

Host mission-critical GN&C FSW processing functions on a spacecraft processor with sufficient computational power and assign sufficient processing priority to execute at the necessary frequency established by analysis.

Discussion:

In virtually all spacecraft, the reliable real-time execution of GN&C FSW on a digital flight computer is an absolute requirement for mission success. In most applications, the GN&C sensor measurement data are acquired and processed on a cyclical basis. These sensor-processing algorithms are mode-dependent and are used to compute the spacecraft's dynamic state. Sensor data is processed by controller algorithms to compute actuator commands, which are then output cyclically to force and torque producing devices. In addition, GN&C FDIR processing must be performed, as well as the GN&C command/telemetry processing functions. All these GN&C real-time software tasks must be scheduled and performed flawlessly at the prescribed cyclic frequencies established by analysis for each mode of operation.

A digital computer, along with its real-time operating system, must be carefully selected by the GN&C developer to adequately perform the scheduling and execution of GN&C processing tasks in such a way that the demanding flight safety critical timing requirements are reliably met with margin. Flight safety critical "hard real-time" processing systems, such as a spacecraft's GN&C system, are different from other processing systems because a failure to satisfy timing requirements may have unacceptable consequences for the mission. These hard real-time systems operate in an environment that has stringent safety and response time constraints.

The result of missing a deadline imposed on a GN&C task execution may be catastrophic. For this reason, there should be a great emphasis early in the design stage on the selection of a digital computer, and its real-time operating system, that can satisfy GN&C processing requirements with demonstrable margin.

A relevant example of this occurred during powered descent of the Apollo 11 LM. A guidance computer related problem occurred that threatened the success of the landing. A previously encountered, but uncorrected, problem in the Apollo 11 LM's rendezvous radar computer interface stole approximately 13% of the computer's duty cycle, resulting in five program alarms and software restarts. The guidance computer had become overloaded and it had more work to perform than processing capability. Reference 33 discusses the root cause for this situation in the context of the operating system for the Apollo flight computers.

Mission and/or Lesson Learned Linkages:

Reference 33

Relevant Questions:

1. What is the estimated GN&C FSW processing computer code, data, and throughput requirement?
2. How will the required GN&C computational power and processing priority be ensured early on within the avionics architectural framework development? When, where, and how will these GN&C computational power and processing priority requirements be addressed throughout the DDT&E process?
3. What is the performance of the computer hosting the GN&C FSW? What is the rationale for the selection of the computer that will perform the GN&C FSW processing functions? What is that computer's spaceflight heritage? What real-time operating system will be employed and what is its spaceflight heritage?
4. Does the GN&C subsystem developer have familiarity with the computer and real-time operating system selected for GN&C processing?
5. Does the GN&C subsystem developer have familiarity with the associated software development and test tools?
6. What are the current estimated margins for GN&C code, data, and throughput? What are these margins predicted to be at PDR, CDR, PER, and at launch?
7. Have minimum acceptable thresholds been set for GN&C code, data, and throughput margins?
8. What are the contractor's corrective action and risk mitigation plans when GN&C FSW margins deviate from the plan?
9. Will GN&C FSW processing functions be performed on a computer solely dedicated to the GN&C subsystem?
10. Will GN&C FSW processing functions be performed on a general-purpose computer that is to be shared between spacecraft subsystems?
11. Does the selected GN&C computer, and associated avionic elements for data transfer, satisfy the GN&C sensor sampling/actuator commanding rate and data latency requirements established by analysis under both nominal and stressed conditions?
12. During testing has the worst case execution time of each GN&C mode been determined and analyzed? If the computer is shared per Question 10 above, how are the worst case requirements/interactions for the other processes emulated/simulated during test?
13. Have on-orbit GN&C FSW maintenance plans and procedures been developed? Will there be a dedicated testbed facility for on-orbit FSW maintenance and support functions? What capability will there be to implement on-orbit code patches?

GN&C Best Practice #5

Ensure that autonomous GN&C fault management is independent of all hardware and software that might be involved in either causing or diagnosing a fault.

Discussion:

The spacecraft should have an independent safe haven attitude control mode to be entered in spacecraft emergencies. Safe haven mode should behave very predictably using components that are completely independent of those used to diagnose the fault. The same sensor (e.g., a gyroscope) cannot be relied upon to monitor the performance of a control loop if it is also used as an element of that control loop. Correct diagnosis is more certain when a diverse set of dissimilar hardware and/or software is used to perform FDIR.

The fault management system (particularly the software) can be a source of single-point failures. Inaccurate situation awareness can lead to wrong disposition. For example, faulty sensor data may create a phantom problem and spoof the fault management system into taking precipitous actions such as resets. Resets must be managed with care to avoid the possibility of becoming trapped in an endless cycle of resets. In addition, a reset during anomalous conditions may reset relays into a dangerous state. Safe hold should ensure that fault protection takes proper action regardless of spacecraft state.

In general, if a fault is detected that may have been caused by a control actuator, then that actuator should be disabled and a functionally redundant actuator substituted for it. For example, if the reaction wheels fail to control attitude then a backup set of thrusters might be used in their place. However, special care must be exercised if a fault is detected during thrusting operations. Any thrusters that may have been involved in causing the fault must be disabled. Fault responses should not be allowed to interrupt critical activities such as Delta V maneuvers. In this particular case, a redundant set of thrusters may be required.

Mission and/or Lesson Learned Linkages:

- Appendix A: Mars Observer, Voyager, FUSE, ERBS, Lewis
- Aerospace LL #18, 35, 36
- GSFC GOLD Rule #1.17
- NASA LLIS #0343, 0345, 0403, 0409, 0625

Relevant Questions:

1. Can a single credible fault (e.g., a failed gyroscope) trigger safe haven entry and then cause safe haven failure?
2. In the event of a fault, will the satellite autonomous management system and the ground controller be provided with correct information? Does safe haven require ground intervention?
3. Can a momentary wiring short in the bus reset all relays into an undesired configuration at any time in the mission? Is the system designed to revert to “last known good state”?
4. Does the fault management design consider all operational possibilities such as solar array mispointing, engine abort, or eclipse transient?

5. Will the fault correction software execute if there is a major anomaly such as a computer freeze?
6. Will the fault management system be tested on the flight spacecraft before launch?
7. Is the fault management system enabled only in those mission phases where it serves a useful purpose?
8. What are the safety positive interlocks in the architecture for inhibiting thruster firings during prescribed “no fire” periods (e.g., during EVAs or during fault diagnosis periods)?
9. What are the system requirements and design drivers that establish the time constraints on entry into safe haven and the maximum time period that safe haven can be maintained?

GN&C Best Practice #6

Establish and flow down the higher level of GN&C requirements necessary for a multi-vehicle system of spacecraft that must safely interact during the rendezvous, proximity operations, docking/undocking, and/or mated operational mission phases.

Discussion:

The hardware and software implementation of a rendezvous capability must be seamlessly architected, integrated, and coordinated between two or more interacting spacecraft GN&C subsystems. The requirements for the individual spacecraft GN&C systems should flow down from the overriding requirements for the coordinated guidance, navigation, and control of the interacting spacecraft.

The requirements, components, algorithms, operational methods and fundamental dynamics of the rendezvous, proximity operations, docking/undocking, and mated operational phases of the mission must be carefully factored into the GN&C architecture as early as possible in the DDT&E process. This is necessary to avoid potential operational complexity, inefficient use of ground system and spacecraft resources, spacecraft collisions while docking or undocking, control system interactions, loss of control authority, and/or dynamic instabilities of mated (stacked) spacecraft configurations.

Due to different inertia properties, control system bandwidth, and pointing requirements following rendezvous and docking the control authority required for the stacked configuration will not necessarily be compatible with that which is required for the individual spacecraft. The effect of stack flexibility on stability may become the dominant design driver if it is necessary to use actuators and/or sensors that are located on different spacecraft modules to control the attitude of the stacked system.

Mission and/or Lesson Learned Linkages:

- Appendix A: DART, MIR, SOYUZ
- GSFC GOLD Rule # 1.01

Relevant Questions:

1. Is the rendezvous trajectory passively safe so that collision avoidance is intrinsic in the event of a sensor, computer, or thruster failure?
2. Does the closing trajectory accommodate dispersions in range, range rate, and cross-track? What is the sensitivity of consumable allocation and the timeline for rendezvous and docking to variations in the dispersions?
3. Is there a seamless transition between autonomous and astronaut control during rendezvous, docking, and proximity operations?
4. Does the GN&C mechanization accommodate astronaut commands that are intuitively based on the human perception of LOS data?
5. How will the individual spacecraft GN&C subsystems interface and interact with each other when mated in a stack?

6. Does the spacecraft GN&C architecture require the inclusion of command, data, and telemetry interfaces to allow the use of GN&C sensors and actuators on different modules while mated?
7. How well will the rigid body mass properties and modal frequencies of the stacked configurations be known in advance and how sensitive is the GN&C system to parameter variations?
8. How adaptive is the GN&C attitude/momentum control system? Is there a provision for a composite (i.e., stacked module configuration) mass properties estimator?
9. Has an analysis of degraded rendezvous sensor functionality and maximum design condition variations been performed and not just an evaluation of complete loss of sensor functionality?
10. Has a minimum fault tolerance level been established for the rendezvous vehicles?
11. Is an independent collision avoidance sensor employed on the rendezvous spacecraft?
12. Do the specifications for the rendezvous spacecraft contain detailed fault detection, isolation, and recovery requirements?

GN&C Best Practice #7

Critically evaluate redundancy with identical GN&C hardware components to ensure that the net effect is an overall increase, rather than a decrease, in system reliability. Always keep in mind that redundancy inherently adds complexity.

Discussion:

Hardware redundancy is used to tolerate hardware failures. However, redundancy is not always desirable in terms of GN&C fault management. If the primary and redundant units share the same current feed, software, or processor, one flaw in the primary component can cause the backup to fail in the same way. A redundant GN&C configuration using unproven components is not a solution. Examples include the experience with the HEAO spacecraft six-gyroscope configuration that experienced failure of all six gyroscopes, and the Hubble Space Telescope, which required several on-orbit gyroscope package replacements.

Only design diversity can mitigate design errors. Diversity uses redundant, dissimilar hardware and/or software and a method to establish which is working correctly. Hardware redundancy does not necessarily protect against software faults. Redundancy of function by a different implementation may provide safer fault management than redundancy with identical implementation.

When designing redundancies into systems, consider the use of nonidentical approaches for backup, alternate, and redundant items. A fundamental design deficiency can exist in both the prime and backup system if they are identical. For example, the rate gyroscopes in the Skylab attitude control system were completely redundant systems, i.e., six rate gyroscopes were available, two in each axis. However, the heater elements on all gyroscopes were identical and had the same failure mode. Thus, there was no true redundancy and a separate set of gyroscopes had to be sent up on Skylab 4 for an in-flight replacement.

Mission and/or Lesson Learned Linkages:

- Appendix A: Mars Observer, Voyager, FUSE, ERBS, Lewis
- Aerospace LL #18, 35, 36
- GSFC GOLD Rule #1.17
- NASA LLIS #0343, 0345, 0403, 0409, 0625

Relevant Questions:

1. Has the use of diverse GN&C components, to provide functional redundancy in the architecture, been traded against the resources that will be needed to source/procure, qualify, test and integrate these additional components?
2. Does the use of diverse GN&C components, to provide functional redundancy, degrade performance? If it does, is the degradation acceptable?
3. Does switching between redundant units ensure a safe transfer for all credible failure paths (e.g., parts failure, start-up transients, latch-up, overvoltage, and electromagnetic interference (EMI), software endless looping)?

GN&C Best Practice #8

Evaluate all heritage hardware and software elements in the GN&C architecture in light of potential differences in build, flight configuration, mission application, flight operating environment, and design/operations teams.

Discussion:

Heritage equipment fielded in an orbital spacecraft mission or aircraft application may not be applicable for use in a crewed vehicle, especially one envisioned for a Lunar or Mars venture. The capabilities may not be consistent with the flight requirements and operational modes. Any operating environment differences are likely to have serious implications. Their implementation in a fail-operational architecture may not be possible or may be complex with vulnerabilities. In the case of the Shuttle Orbiter, the original selection of the inertial system was derived from the heritage experience of the KT-70 system fielded in tactical aircraft applications. Incompatibilities in equipment capabilities and environmental provisioning required extensive redesign resulting in essentially a customized configuration called HAINS, or High Accuracy Inertial Navigation System.

In some applications, the use of a tactical GPS selection was inconsistent with space environment conditions and software limits on the velocity range and codes, etc. were realized only after commitment to a component. The initial selection of the Shuttle computer based on the tactical "4-pi Processor" resulted in initial reliability problems and limitations in the fault tolerant implementation. Reliability and memory limitations led to an upgrade to an AP101S in later Shuttle usage. Changes introduced to meet performance operational requirements have to be fully validated to assure that reliability objectives are met. More intense analysis and test may have resulted in a different component selection or demonstration of satisfactory change achievement and reliability at lower cost before commitment to the heritage unit.

Any change in the application of previously developed hardware, software, or operational procedures may require a certain amount of redesign to ensure proper functionality in the new circumstances. For example, fault management circuits may need to be redesigned because when a heritage unit is scaled up, key parameters such as start-up current and rise time may change. Some changes may require complete re-qualification of the heritage component or process.

Design upgrades made while an old unit sat on the shelf should be considered if an old unit is being re-commissioned for flight. It is not sufficient for the replacement parts or units to merely meet lot acceptance specifications. Component qualification must be based on sufficient engineering data. That a few items worked is not sufficient—statistical data may be required to show margin of safety.

Removal of obsolete portions of the code should be considered if legacy software is being reused. Software reuse should be thoroughly analyzed to ensure suitability in a new environment, and all associated documentation, especially assumptions, should be reexamined. Extensive testing, including software loop and path testing, should be performed at every level, from unit through system test, using realistic operational and exception scenarios.

Ariane Flight 501, which took place on June 4, 1996, was the first test flight of the Ariane 5 expendable launch system. As described in reference 38, it resulted in a complete failure. Due to

a malfunction in the flight control software the rocket veered off its flight path 37 seconds after launch. It was torn apart by high aerodynamic forces caused by excessive TVC commands from the launch vehicle's onboard flight computer. The breakup caused the loss of the payload: four Cluster mission spacecraft, resulting in a loss of more than $370 million. The Ariane 5 software reused the specifications from the Ariane 4, but the Ariane 5's flight path was considerably different and beyond the range for which the reused code had been designed. Specifically, the Ariane 5's greater acceleration caused the backup and primary inertial guidance computers to crash, after which the launcher's nozzles were directed by spurious data. The inertial reference system of Ariane 5 is essentially common to a system that flew on Ariane 4. The part of the software that caused the interruption in the inertial guidance system computers is used before launch to align the inertial reference system and also, in Ariane 4, to enable a rapid realignment of the system in case of a late hold in the countdown. This realignment function, which served no purpose on Ariane 5, was nevertheless retained for commonality reasons and allowed, as in Ariane 4, to operate for approximately 40 seconds after lift-off. Pre-flight tests had never been performed on the re-alignment code under simulated Ariane 5 flight trajectory conditions, so this software reuse error was not discovered before launch.

Mission and/or Lesson Learned Linkages:

- Appendix A: Landsat-6, Genesis, Lewis
- Aerospace LL #87, 95
- NASA LLIS #0310, 0625, 1370
- Reference 38

Relevant Questions:

1. Has a heritage review been conducted to assess and document how the requirements, environments, lifetime of the present mission, compare to capability of the heritage hardware and software?
2. Have all heritage equipment test and flight anomalies been resolved?
3. Have catastrophic failures that involved similar technologies been reviewed?
4. Have replacement materials and parts used in heritage equipment been fully qualified?
5. Is the heritage hardware being assembled in exactly the same manner as the original or is it being built to print by some other process that may not be the equivalent of the original?
6. What is the requalification plan and process if the original hardware or software is being reused?
7. Under anomalous circumstances, is it possible for obsolete segments of legacy code to be executed?
8. Has the "heritage" of the unit being considered been analyzed for relevancy to the current mission application, especially in terms of the operating environment, parts, life, and intrinsic characteristics?

GN&C Best Practice #9

Make certain that new GN&C technology is well qualified. It must have sufficient statistics to show an acceptable safety margin, and flight-proven alternatives must be identified.

Discussion:

Emerging GN&C technology has the potential to allow space missions to be performed more affordably, safely, reliably, effectively, and in new operational regimes. This technology promises either to provide GN&C performance previously unattainable, or to provide the same level of performance with fewer resources than previously required.

Currently there are multiple GN&C related items in the technology pipeline (e.g., MEMS inertial sensors) at various levels of TRL maturity. However, there are very limited flight opportunities for any of these GN&C technologies to be validated on-orbit. It can be assumed that any technology assessed to be at a state less than TRL 7 (i.e., Prototype Demonstrated in Space Environment) will require significant funding and schedule resources to attain "flight qualified" status. Inclusion of emerging GN&C technologies (any item objectively evaluated to have a TRL less than 7) should be carefully considered, justified with a strong engineering rationale for its infusion, and carefully planned.

An example of this in the GN&C arena was the premature adoption in the mid-to-late 1980s of RLG technology as a substitute for the traditional spinning mass "iron" mechanical gyroscopes in some spacecraft attitude determination and control applications. The transition of the RLG technology was based upon the favorable insertion and performance of the RLG technology in inertial navigation systems for terrestrial, airborne, and marine military platforms. The point is that when first infused into NASA space missions the RLGs were a non-space qualified technology. RLGs had not attained TRL 7 (i.e., prototype demonstration in an operational environment) in the space environment although it was in broad operational use (TRL 10) in the aforementioned terrestrial, airborne, and marine applications. In retrospect, life tests and better qualification may have prevented numerous on-orbit anomalies and failures with this RLG technology [ref. 59].

Mission and/or Lesson Learned Linkages:

Reference 59

Relevant Questions:

1. What GN&C technologies, with TRL less than 7, have been considered and why? What technology cost/risk/benefit trades have been performed?
2. What specific GN&C technologies have been incorporated into the GN&C baseline architecture? What is the engineering rationale for their inclusion?
3. What is current TRL of each GN&C technology? What TRL is needed at PDR, and at CDR? How much time is in the Project schedule to reach these maturity gates? What is the Delta-TRL per project year metric for each technology being infused?
4. Has a GN&C Technology Development Plan been formulated?

5. Have technology readiness gates and objective criteria been formulated to meaningfully assess technology advancement, and have they been included in the GN&C Technology Development Plan?
6. Is the GN&C architecture such that one new technology relies on another new technology in order to achieve the desired flight performance?
7. What project resources have been allocated to permit infusions of GN&C technologies?
8. What assumptions has the prime contractor made in the rate of GN&C technology maturity?
9. What is the spacecraft prime contractor's level of familiarity with each selected GN&C technology?
10. Was the technology developed "in-house" by the prime contract or is it being secured from an external source via sub-contract or partnership? What is the quality of the relationship (both from a technical and from a business perspective) between the prime spacecraft contractor and the GN&C technology provider? Have they successfully collaborated on technology infusions in the past or not?
11. How is the technology development being funded: vendor is funding it out of IR&D, the vendor has another government or commercial entity funding the development, another NASA project or program is funding it, or it is being funded by the current project? How much control does the project have over the funding, and what risk funding has been planned?
12. Is the GN&C new technology dependent on the development of a flight-qualified component by a third party (e.g., detector, processor, memory)? How much control does the project, prime, or subcontractor have over this development?
13. Does the GN&C implementation plan include provisions for pre-planned higher-TRL (or ideally, flight-proven) alternatives that addresses the risk posed by the failure of a baselined low-TRL technology to mature consistent with the project schedule? Have both the GN&C subsystem-level and the spacecraft system-impacts of reverting to these flight–proven alternatives been assessed?
14. When the prescribed GN&C technology readiness gates are not met for critical technologies, is the project prepared to cease development and implement preplanned alternatives in a timely and efficient manner?
15. Have qualification criteria for a new technology been carefully researched to ensure that there are not different measures of effectiveness and inherent new problems (e.g., helium poisoning of hemispherical resonator gyroscopes) with the new technology?

GN&C Best Practice #10

Adhere to a Design for Test philosophy: Consider the degree of difficulty of performing ground validation testing and pre-flight calibration when evaluating candidate GN&C subsystem architectures.

Discussion:

Design for test and the adequacy of the test capabilities often is an afterthought in design. Involvement of the test engineers in the design process enables definition of needed data interfaces and readouts that evidence both satisfactory operation and trending as well as failure isolation and often failure prediction capabilities. Early definition of test requirements provides a sound basis for test facility development and timely equipment readiness.

Making design provisions for test as an afterthought leaves uncertainties in function and increases the difficulty of isolating a failure mechanism in an integrated system. Special one-of-a-kind test configurations (e.g., break out boxes and digital waveform analyzers) implemented during the validation testing phases may allow extensive data access but cannot (and should not) be carried forward in the full-up system flight configuration. Similarly an over emphasis of the hardware test point concept is difficult to be realized in a flight configuration and may be undesirable. The Block I Apollo GN&C hardware configuration implemented extensive test point connectors in the hardware elements and was only consistent with an ad-hoc debugging process, which introduced possible failure modes. This cumbersome and risky method was abandoned in the Block II flight hardware. Instead, Block II relied on availability of a telemetry data stream and key performance indicators. In this improved Block II design, sufficient data was therefore made available and was safely buffered to support testing activities.

In summary, test planning and implementation consistent with the use of the flight system's telemetry downlink is most desirable for supporting both ground pre-launch checkout testing and flight operations. Spacecraft telemetry systems should be designed to be configurable for high-rate "every cycle" GN&C data capture and output for use in ground test verification and troubleshooting.

Mission and/or Lesson Learned Linkages:

References 2, 3, 4

Relevant Questions:

1. Is the contractor planning to define GN&C test requirements and design/build the required GN&C test facilities concurrently with design effort?
2. Is the contractor planning to use existing special purpose GN&C test facilities/equipment? If so, have they been shown to be adequate, operational, and available, or has the contractor planned resources to upgrade, retrofit, and calibrate the facilities/equipment?
3. Is there evidence that GN&C test engineers are involved in the GN&C design process to enable definition of needed data interfaces and readouts that will indicate both satisfactory subsystem operation and trending as well as failure isolation?
4. Does the contractor plan for early definition of GN&C test requirements?

5. What is the basis and rationale for test facility development?
6. What evidence is there that the proper planning has been done to ensure timely test equipment readiness?
7. Has there been an effort to minimize the need for non-flight GN&C special test equipment, test fixtures and associated Ground Support Equipment (GSE)?
8. What GN&C testing can be performed at the fully integrated spacecraft level prior to shipment to the launch processing facility at the launch site? What are the specific limitations to GN&C testing at this point in the spacecraft development?
9. What GN&C testing can be performed at the launch processing facility? What are the specific limitations to GN&C testing at this point in the spacecraft pre-launch processing?
10. If the fully tested flight ready GN&C subsystem hardware/software configuration is altered what is the contractor's approach for re-test?

GN&C Best Practice #11

Define and document the coordinate frames and the system of units (and associated conversion factors) that are to be employed, and rigorously enforce compliance.

Discussion:

The use of a common set of units and coordinate frames is necessary to prevent miscommunication of technical information. The result of miscommunication can vary in severity—from a delay in schedule to resolve any discrepancies to the cost of reworking ACS components, or to (in the extreme) un-recoverable mission failures due to ACS design errors.

Two systems of units are in common usage in U.S. space programs: metric and English. Individual groups, even within the same company, may use different systems of units because they normally support different customers. The project-level SE is responsible for specifying a consistent set of units that will be used throughout the project. The project SE may permit a parameter to also be expressed in a second set of units inserted parenthetically after the standard units, if doing so will improve understanding.

Similarly, a great number of coordinate reference frames that are used in the development of space systems. Different disciplines will naturally use different reference frames for detailed analyses of orbit mechanics, attitude control, launch loads, etc. Each of the discipline reference frames must have a clearly defined origin of coordinates and orientation with respect to an established standard.

It is sound engineering practice to generate and maintain a project-controlled document that captures the following GN&C items:

- The system of units.
- Definition of all coordinate frames.
- Definition of attitude parameterization (e.g., an Euler angle sequence or quaternion nomenclature).
- Definition of symbols for the GN&C variables and parameters.
- Mission-specific definitions for terms such as “ephemeris,” “bandwidth,” “pointing accuracy,” “pointing stability,” “jitter,” “smear,” “products of inertia,” or “quaternion,” and “targeting.”
- The identification of industry-standard models or databases to be used in analysis and/or simulation (e.g., the JGM3 20x20 gravity model or the Harris Priester atmosphere with solar diurnal bulge).
- Definition of all time references, conventions, and epochs.
- Definitions of the GN&C sensor and actuator coordinate frames.
- Definition of all mission critical GN&C sensor, actuator, or other component alignments.
- Definition of all sensor-to-actuator phasing.
- Definition of all sign conventions, including definition of signs of products of inertia.
- Error budgets for all GN&C mission modes.

Mission and/or Lesson Learned Linkages:

- Appendix A: MCO, AQUA
- Aerospace LL #60, 73, 80

- NASA LLIS #0641, 0692

Relevant Questions:

1. What document specifies the set of units and coordinate frames to be used on this project?
2. Are all of the groups that exchange information in inertial coordinate systems using the same true of date, mean of date, or J2000 reference frames?
3. Is the transformation between the different discipline reference frames unambiguously defined in terms of their relative orientation and locations of origin?
4. If dimensionless units are used (e.g., in software) are the normalizing factors identified with their dimensions?
5. What prefixes are permitted for dimensions (e.g., can both centimeters and millimeters be used)?
6. Is there a defined spacecraft time reference, or explicit set of time references, to be used for the mission in question (e.g., UTC, UT1, GPS time, leap seconds)? Have all such time references been documented?

GN&C Best Practice #12

Ensure controller designs meet or exceed the following gain and phase margin stability criteria as a function of GN&C design maturity.

Stability Margins:

State of Design Maturity	Gain Margin	Phase Margin
Continuous analysis during preliminary design phase	12 dB	45°
CDR-level sampled data analysis with actual FSW digital implementations and final flexible body models	6 dB	30°

Damping Ratio:

For the purpose of analysis and simulation of typically fastened (i.e., bolted or pinned) spacecraft structures, the damping ratio of all flexible body modes shall be assumed to be no greater than 0.1% of critical damping unless analysis or test data demonstrate otherwise. However, for those missions where high-precision spacecraft/instrument line-of-sight pointing is required and low-amplitude jitter-causing vibrations are critically important, the damping ratio of all flexible body modes shall be assumed to be no greater than 0.05%, unless analysis or test data demonstrate otherwise. In extreme cases, such as ultra-low temperature cryogenic space platforms, the use of a damping ratio in flexible body analyses of greater than 0.01% should be justified with test and/or analysis data.

Gain Stabilization:

Control laws and loop compensation shall gain-stabilize all flexible-body modes, except in special cases where gain-stabilization is shown to be a severe design driver. The peak amplitude of each gain-stabilized flexible-body mode shall not exceed -12 dB in the control system open-loop frequency response.

Phase Stabilization:

Flexible-body modes that do not meet the gain-stabilization requirement above shall have phase margin of at least 60 deg over a modal frequency variation of ±25%, with worst-case time delays included.

Discussion:

The Gain Margin and Phase Margin indicate the degree of stability that a system possesses. The gain margin is the change in open-loop gain that will cause the closed loop system to become unstable. Similarly, the phase margin is the change in open-loop phase shift that will result in instability of the closed loop system. Mathematically speaking, and as can be found in any introductory textbook on feedback control theory, the gain margin is the amount of open-loop gain change (usually expressed in dB) that will result in instability when the open-loop phase is –180°. The phase margin (usually expressed in degrees) is the amount of open-loop phase lead or lag that will result in instability when the open-loop gain is 0 dB.

The requirement on stability margins is imposed to guarantee stability of the control system in the presence of uncertainty. The uncertainty decreases as the knowledge of the system and the

sophistication of the analysis improves; this permits a reduction in the stability margin requirements as the design matures.

Data latency in issuing commands to the control system actuators contributes phase lag to the feedback control system that must be accounted for. In this regard, a good practice is to assume a latency of one control computational cycle time interval unless it is known that the latency is greater than one computational cycle. If this is the case, then round up the latency to the next highest integer number of cycles.

A good design practice is that at CDR, the gain margin should be at least 6 dB and the phase margin should be at least 30 deg. Typically by CDR, sampled data stability analysis has been performed using actual FSW digital algorithms and the final flexible body models.

Controls-Structures Interaction:

Actual spaceflight experience has shown detrimental closed-loop coupling between the resonant elastic modes (i.e., the flexible bending modes) of spacecraft structures and the feedback control systems used to stabilize and orient the spacecraft. This is often referred to as the controls-structures interaction (CSI) problem, and it occurs because spacecraft structures are both "light-weighted" and composed of large flexible elements or appendages. For example, the Orbiter experienced CSI issues with its Remote Manipulator System (RMS) robotic arm control system used for Shuttle payload maneuvering. Undesired dynamic interaction between robotic arm, the attached payload and the Orbiter's thruster based Flight Control System (FCS) occurred due to the easily excited, low-frequency and lightly damped flexible modes of the RMS structural dynamics. The operational solution was to place limitations on the envelope of combined RMS/FCS operations and to intentionally slow down RMS angular rates during payload maneuvering operations [ref. 44].

There is a rich set of literature on the CSI problem; a few of the key references are captured as references in this report. Reference 47 (Section 2.1) provides a tutorial-like introduction to the fundamentals of CSI including a description of an iterative design and analysis process. References 68 and 69 provide some informative Apollo-era perspectives on the effects of structural flexibility on vehicle control system, from both the GN&C and Structures engineering viewpoints. Reference 70 provides an excellent fundamental understanding of the CSI problem as it applies to the design of complex spacecraft and pointing system servo loops, using the Jet Propulsion Laboratory (JPL) Pathfinder gimbal pointer as an example application.

Because of uncertainty in the spacecraft structural model, a good design practice is that all flexible modes must be gain-stabilized with a margin of 12 dB to avoid putting energy into the flexible modes. This "flexible margin" requirement means that the resonant peaks of the open-loop flexible modes must be small enough (12 dB is equivalent to a factor of 4) such that the system is stable for any phase change at the flexible mode frequency. Gain stabilization is usually realized through a combination of natural damping and by selecting the bandwidth of the control loop sufficiently smaller than the first bending mode frequency. However, for lightly damped systems, this approach may overly constrain the control loop bandwidth such that pointing performance requirements cannot be met. In that event, the design engineer may resort to phase-stabilization to actively damp out the flexible modes. Phase stabilization means deliberately introducing enough phase lag such that the phase is far enough away from the -180 degree point so that the flexible mode will be stable for any gain.

Proper and sufficient structural modeling plays a critical role in performing CSI analyses. The spacecraft/flight system structural finite element model (FEM), typically developed by Structures team and then delivered to GN&C team, will be used by the controls analyst to study and assess flexible body effects on attitude controller stability. The level of FEM detail and maturity have significant impact on the stability analysis. Structural design iteration with control design is not uncommon, so one should plan for it. The controls analyst should also perform due diligence in assessing the delivered FEM before using it in the controller stability analysis. Reference 67 provides a verification procedure for FEMs developed using the industry-standard MSC/NASTRAN structural analysis tool.

When performing controller stability analysis, it is good practice to simultaneously vary the frequency and the amplitude of all flexible modes due to uncertainty in the spacecraft structural FEM. The application by GN&C engineers of so-called Model Uncertainty Factors (MUFs) has been common practice for decades. These MUFs add conservatism to pre-launch predictions of flexible body dynamics, as represented in the FEM. Generally, the size of the MUFs used by the controls analyst in the stability analysis will diminish as the flight system hardware matures. As the flight system model matures through the execution of component-level and subsystem-level dynamic testing and model correlation, the magnitude of the MUFs can decrease as uncertainty decreases and confidence in the FEM increases. This decrease in the MUF with increasing modeling details and test correlation is often referred to as MUF "burndown." Reference 31 (Section 2.1) provides a good description of MUFs and recommends several guidelines for their application.

Spacecraft engineering organizations and flight project teams often do not have well defined, established, and consistent MUF policies to use at the start of the CSI analysis process. This can lead to inconsistent application and stacking of MUF's potentially resulting in over conservative predictions of stability margin impacts due to flexible body dynamic effects.

Even a test-correlated structural FEM may have model versus flight system hardware frequency variability in "major modes" of ±5%, while preliminary models will certainly have much more variability. Early in the design phase, the control loop stability analysis should show robustness to variations of +/- 10 % in the lowest frequency modes and +/- 25 % in the highest frequency modes. This is because typically, the uncertainty in the modal data output from the structural FEM increases with frequency. The preliminary structural FEM that is constructed early in the spacecraft design process must be of sufficient order and modeling fidelity to accurately predict the lowest modal frequencies (e.g., the first two or three bending mode frequencies) to support preliminary control system stability analysis. Obviously this early FEM should capture the dynamics of the fully-deployed on-orbit spacecraft flight configuration. Subsequently, later in the spacecraft design process, higher order structural FEMs must be formulated to accurately predict the properties of the higher frequency flexible modes. As the spacecraft design matures the uncertainty in modal frequencies should diminish as more sophisticated structural FEMs are developed and as modal test data becomes available to refine the model.

As a side note, it would behoove the control engineer to have an understanding of how the spacecraft structural FEM was assembled and validated. In particular, the control engineer should understand the uncertainty in the coupling terms used in the FEM to represent joint and hinge type mechanical attachments between the spacecraft structural subassemblies. The nature of these coupling terms can strongly influence modal frequency predictions. For example, a

“hard” hinge stiffness in a deployed solar array would produce upper bound on modal frequencies whereas a “soft” hinge stiffness would produce lower bound. The assumptions made by the structural engineer concerning coupling terms in the FEM must be clearly identified and documented for the benefit of the control engineer.

In a gain stabilized control loop, the selection of a controller bandwidth that is sufficiently large to meet pointing performance requirements often imposes a hard limit on the lowest allowable spacecraft flexible mode frequency. In practice, it is very common for the control engineer to levy a specific written requirement on the spacecraft structural engineer to ensure the first bending mode frequency of the vehicle (including all its flexible appendages) is above a minimum value (e.g., 0.3 Hz). Typically this minimum value is negotiated based upon a compromise between the desired controller bandwidth needed to satisfy performance requirements and the realities of lightweight space vehicle structural design practices.

Notch filtering is a specific type of gain stabilization that the design engineer can employ, but only with caution because of the aforementioned uncertainty in spacecraft flexible mode frequencies. Fundamentally a notch filter is a narrow band-reject filter that sharply attenuates (i.e., “notches out”) the modal gain in a control loop associated with a single flexible mode. Therefore notch filtering is sensitive to variations in modal frequency. It should only be used when confidence in structural modeling is high because a notch filter transfer function is deliberately “tuned” to suppress oscillations of a single flexible mode. A particular notch filter has little influence on other flexible modes, which occur at different frequencies.

A real world case that illustrates the challenge to the control system designer in dealing with both the uncertainty in flexible mode frequencies and the sensitivity of the notch filtering approach can be found in reference 40, which highlights a Gemini/Agena TVC system design issue. When mated on-orbit, following rendezvous and docking, the Gemini/Agena stack was a single, large, flexible body composed of two individual spacecraft joined at the structurally flexible docking interface. Concerns were raised regarding the TVC controller stability while performing mated orbit-changing maneuvers by firing the Agena main engine. Early preflight analysis revealed inadequate TVC gain margin in the presence of an estimated 5-Hz first bending mode during propulsive maneuvers. Since lowering the control bandwidth was not an option the TVC designers initially elected to employ a gain stabilization approach that entailed a notch filter set for maximum attenuation at the predicted 5 Hz first bending mode frequency. Analytically this approach provided the desired 6-dB gain margin in the TVC loop. However, subsequent study revealed the first bending mode was actually closer to 3 Hz than the previously predicted 5 Hz. This revelation led to a re-design of the TVC control system loop compensation. The Agena TVC stability margins were subsequently achieved by adopting lead/lag compensation. It is interesting to note that subsequent Gemini/Agena ground test results indicated the first bending mode frequency was at 3.6 Hz and whereas the actual in-flight test data indicated the mode to be approximately 10% higher at 4 Hz.

The point to be emphasized here is that notch filtering is a gain stabilization technique that must be judiciously applied in those cases where the designer does not have the leeway to simply lower the control bandwidth and does not desire to employ phase stabilization methods. Notch filtering is most appropriately applied relatively late in the design cycle when there is a high level of confidence in the spacecraft flexible mode frequencies. This confidence is typically achieved with CDR-level high-fidelity structural FEMs anchored with relevant modal test data.

It is good control system engineering practice to compare the stability robustness results obtained from the linear frequency domain analyses with those obtained from the non-linear time domain simulation of the system dynamics. Typically, the time domain simulation is used to generate pointing performance predictions but it can also be exploited in a relatively straightforward manner to perform a "sanity" crosscheck on both the gain margin and phase margin values determined from Bode (or Nichols or Nyquist) stability analysis. The gain margin can be crosschecked by simply increasing (or decreasing) the parameter in the time domain simulation that influences the system's loop gain until a point of instability is reached. Similarly, the phase margin can be checked by increasing the time delay parameter in the time domain simulation until a point of instability is reached. Obtaining close agreement between the stability robustness values obtained from the frequency domain and the time domain approaches is highly advisable. However agreement between these two sets of stability robustness values may be difficult to achieve for non-linear, high-order, dynamically complex systems.

The stability guidelines given above are intended for single input-single output (SISO) control systems that are operating in a steady state. However, a control system design may be perfectly acceptable even if it does not satisfy the steady state criteria during all time periods, particularly if the duration of non-compliance is relatively short compared to the response time of the vehicle dynamics. Consider a three-axis-controlled spacecraft in a polar LEO. If the attitude sensing is provided by magnetometers and Sun sensors, then the attitude reference about the third axis will be lost whenever the magnetic field vector and the Sun vector line up. Since the pointing error about this axis is temporarily unobservable, the attitude drift is restrained by inertia or momentum bias rather than active control. In this case, the magnetic field vector changes direction on the order of a tenth of a degree per second as orbital motion moves the spacecraft away from the singularity. Three-axis attitude determination and control will be restored within a few hundred seconds at most. Likewise, a related situation may occur if the gain margin is degraded temporarily due to a mismatch between environmental torques and the available control authority. This second situation may occur in orbiting spacecraft that use magnetic torquers or in launch vehicles passing through the point of maximum dynamic pressure (i.e., the Max Q point).

As described above the conventional approach to solving spacecraft CSI problems has been to use SISO frequency-domain control loop shaping compensation techniques to achieve desired controller flexible body stability margins. This approach often results in a performance-limited design where the controller closed-loop bandwidth is purposely constrained to be well below the first bending mode frequency. When implemented properly, this conventional SISO approach of trading stability robustness for bandwidth limited performance has been flight-proven on many NASA spacecraft and shown to work well for most mission applications to date.

Multivariable Multiple-Input/Multiple-Output (MIMO) Stability Robustness Analysis:

The classical SISO control-loop-shaping compensation design approach breaks down, however, for spacecraft applications that require high bandwidth control in the face of multiple clustered lightly damped structural flexible modes of vibration. This type of controller design problem may, for example, present itself on large, structurally complex space platforms assembled on-orbit by mechanically linking multiple lightweight sub-elements. For these very demanding mission applications, the control system designer will need to exploit one or more of the many multivariable MIMO-based design techniques that have been developed since the 1960s. In fact,

some existing, and many emerging space platform control systems, are of multivariable MIMO nature and consequently are not amenable to the classical SISO frequency domain stability robustness analysis techniques of Bode [ref. 45], Nyquist [ref. 46], and Nichols [ref. 47] (and, the time domain root locus analysis method of Evans [ref. 48] as well for that matter) that all date back to the 1930s, 40s and 50s.

Reference 42 discusses the challenges and barriers to the implementation of multivariable control systems. Garg provides valuable insight into ways of overcoming these challenges and emphasizes that the robustness determination of MIMO control systems requires complicated analyses using, for example, combinations of singular value techniques and Monte Carlo simulations.

Many researchers have labored, with varying degrees of success, to develop modern stability robustness evaluation methods for MIMO control systems. A detailed discussion of these MIMO methods is beyond the scope of this report but a brief survey will be provided here for background and insight.

In the 1960s and 70s, there were attempts to extend the established SISO techniques to MIMO applications with mixed results. Some developed ad-hoc methods to adapt SISO methods for MIMO stability analysis in which gain/phase margins are computed sequentially one loop at a time. These "one-loop-at-a-time" approaches have weaknesses and are not uniformly reliable ways to predict MIMO control system stability. Clearly these methods are unsuited for MIMO control systems with strong loop interaction, or where it is very difficult to understand and decouple complex input/output relationships.

Reference 41 describes the comparison of stability analysis results obtained for a fully coupled 6-DoF linear model of a missile flight control system using the SISO method and the multivariable gain and phase margin method. Disturbingly, the findings reported in this paper indicate that the multivariable stability margins decrease with the missile's total angle of attack, whereas the classical SISO margins exhibit little to no dependence on the total angle of attack. Close agreement between the multivariable and SlSO stability margins occurs only at very small values of total angle of attack where the missile's equations of motion are lightly coupled. As reported in the conclusions of this paper, as the total angle of attack increases, the vehicle's dynamic coupling also increases, and the multivariable margins decrease. This degradation in stability margins is not seen in the results of the SlSO analysis. Thus, we have here an example of the fact that for highly coupled dynamic systems having acceptable SlSO margins is not a guarantee of satisfactory multivariable margins.

A high level historical survey of this MIMO stability topic reveals that in the mid-1960's Zames [ref. 49] developed a small gain theorem for studying unstructured perturbations in multivariable control. This initial work was soon followed by Postlethwaite's [ref. 50], MacFarlane's [ref. 51], and Rosenbrock's [ref. 52] pioneering developments in the 1970s to extend the classical SISO frequency domain techniques and the root locus to MIMO control systems. In the 1980s, Doyle [ref. 53], Stein [ref. 54], Athans [ref. 55], Laub [ref. 56], and Safonov [ref. 57] all pursued the development of modern processes and tools to solve the robust multivariable controller design problem. In particular, they researched techniques to combine the best of the classical SISO methods with the more mathematically sophisticated modern state space optimal control theory of the 1960s and 70s. What emerged was a new approach that computed and displayed MIMO

stability margins based upon the singular value properties of the system's loop transfer matrix (LTM). Effectively, the gain and phase margins of a MIMO control system could be portrayed with plots of the LTM's minimum and maximum singular values versus frequency. This technique was the multi-loop extension to, and analog of, the classical single loop frequency domain graphical techniques. Therefore practitioners of the classical SISO Bode method could directly relate to and intuitively interpret the multivariable singular value plots.

The development of advanced multivariable MIMO control system design and analysis methods continued in the 1990s and beyond, building upon the results of most all the researchers named above. The subsequent work in this area led to the development of systematic multivariable loop-shaping design methods to synthesize realizable MIMO controllers, which met performance objectives while guaranteeing robustness against model uncertainty. Several of these MIMO techniques that were matured in the late 1980s and 90s (e.g., H_{oo} synthesis, μ-analysis and linear matrix inequality optimization) are currently being used by designers of multivariable controllers.

Liquid Propellant Slosh Dynamics Considerations:

Launch vehicle flight control and spacecraft attitude control engineers have long been aware of the challenges of adequately addressing the potentially de-stabilizing effects of liquid propellant slosh dynamics [ref. 36 and 37, Section 2.1]. Historically speaking, the first observed incident with propellant slosh occurred on the second flight of the Jupiter launch vehicle during which stepped-pitch guidance commands were issued at a frequency near the liquid oxygen slosh mode frequency with the unfortunate consequence of the vehicle being lost during ascent at the point of maximum dynamic pressure [ref. 38, Section3.1].

Sloshing is a complex nonlinear dynamic phenomenon but, simply put, sloshing can be considered as the periodic motion of the free surface of liquid in a partially filled propellant tank. Propellant sloshing can occur on either a launch vehicle or on a spacecraft. The focus in this section will be on considerations of slosh dynamics for spacecraft rather than launch vehicles.

Sloshing can be induced by a vehicle's rigid body dynamic response to attitude control system commands or from abrupt changes in a vehicle's acceleration profile. In the latter case these changes in vehicle acceleration can occur at the end of an active thrusting period or, in the case of a launch vehicle, when encountering wind gust during the ascent phase of flight. The sloshing liquid mass, if unconstrained, can impart disturbance forces and torques internal to propellant tank. In a closed loop attitude control system these slosh disturbances can deleteriously couple with a spacecraft's rigid and flexible body dynamics leading to a potential instability.

In extreme cases slosh induced instabilities could lead to vehicle structural failure due to excessive loads. Slosh could also cause the premature shutdown of engines/thrusters (or an inability to start engine/thruster operation) if the sloshing liquid motions preclude the normal flow of propellant out of the tank.

Slosh is an inter-disciplinary problem requiring the GN&C engineers to closely collaborate and consult with their counterparts from the propulsion discipline for the development of appropriate slosh dynamics models. This is similar to the relationships formed between the GN&C discipline engineers and the structures discipline engineers for the modeling of the flexible body dynamics. Typically, as is done for the modeling of the spacecraft's flexible body modes, conservative

values for the open-loop slosh mode damping are used for the stability analyses of a spacecraft's attitude control system or a launch vehicle's flight control system.

The 1966 NASA Special Publication SP-106 is an outstanding comprehensive monograph on the fundamentals of the dynamic behavior of liquids in moving containers [ref. 39, Section 2.1]. It summarizes almost all of the early work done on slosh modeling and is still to this day commonly used by engineers seeking to understand the motions of liquid propellants contained in launch vehicles and spacecraft. In 2000 an updated slosh modeling document was issued by Southwest Research Institute that emphasized the most recent research and literature at the time on slosh modeling and analysis and provides the results that are of most interest for spacecraft applications (ref. 40, Section 2.1]. Readers that have an interest in slosh modeling should obtain copies of both these seminal references.

A recurrent theme historically seen in slosh-induced anomalies and/or failures is either non-existent or insufficient slosh modeling. Often Computational Fluid Dynamics (CFD) modeling is used to support the formulation of the slosh dynamics model [ref. 41,Section 2.1]. Also, slosh ground testing is conducted using flight-like tanks to support the development of slosh dynamics models. The GN&C engineering team should strongly consider employing CFD modeling and ground testing, especially for cases where the complexity of the slosh dynamics is a driver.

Often the liquid propellant tanks used on spacecraft have bare walls which can result in more pronounced slosh effects. In other cases, the propellant tanks they may have internal diaphragms or bladders, or other forms of PMDs, anti-slosh baffles, or other types of slosh suppression devices [ref. 42, Section 2.1]. Of course, these slosh suppression devices add mass to the spacecraft which is a system-level consideration. The obvious advantage of using these devices is their influence on the slosh mode damping values. For example, on the NASA/GSFC Solar Dynamics Observatory, the non-PMD (i.e., bare wall tank) case that was analyzed had a slosh mode damping ratio of 0.2% whereas the PMD case had a dramatically increased damping ratio of 8.0% [ref. 43, Section 2.1].

Thus, for spacecraft carrying relatively large amounts of propellant for thruster-based orbital insertion, orbital maneuvering, and/or reaction wheel momentum unloading, it is imperative that the impact of slosh dynamics, on both spacecraft attitude control performance and stability, be well characterized and understood. Slosh effects must therefore be carefully accounted for in a spacecraft's attitude control system design. To determine the need for a slosh analysis a very simple rule of thumb can be based upon the ratio of the propellant mass to the spacecraft dry mass at the start of the mission. For the case when that ratio is greater than 20% to 30% a slosh analysis (and the attendant development of a slosh model) be performed. This is needed since a poorly designed attitude controller design could potentially excite the slosh dynamics phenomenon, which can adversely impact performance and stability. All attitude control modes should be analyzed for slosh dynamics impacts, especially those modes employing RCS engines/thrusters for control torque actuation or for performing Delta-V maneuvers. It is important for the GN&C analyst to perform sufficient modeling, simulation, and analyses in order to well understand the degree of dynamic coupling between the liquid propellant slosh modes and the spacecraft's flexible body modes.

Historically, starting in the early 1960s, the work on slosh dynamics was confined to relatively high axial acceleration launch vehicle ascent and orbital insertion flight control applications.

Such applications have high Bond numbers; the Bond number being the parameter of most importance here. The Bond number, Bo, is a dimensionless indicator of dynamic fluid phenomena. Refer to Appendix G for the simple equation used to actually compute the Bond number. More specifically the Bond number is a measure of the relative importance of surface tension to gravitational forces and it is used to describe the transition of a liquid to a gravity dominated flow. GN&C analysts use the Bond number to distinguish between low-g and high-g slosh regimes. Again, maintaining the focus in this section on spacecraft attitude control versus launch vehicle flight control applications, the low-acceleration (low-g) slosh regime is of most interest here.

The widely held perception in the CoP is that the high-g slosh dynamics problem (where Bo > 1000) has more-or-less well-established solutions. There exist extensive test-correlated analytical models for commonly used launch vehicle geometries. In particular there are the well-known spring-mass mechanical models and the pendulum mechanical models that have been widely applied to the high-g launch vehicle slosh problems with very good results obtained.

Conversely, the low-g slosh dynamics problem (~30 < Bo < 1000) is still in need of more attention to formulate feasible and accurate solutions. Reference 40 (in Section 2.1) captures information on the lateral sloshing of liquids in axisymmetric tanks under low-gravity conditions and also provides equivalent mechanical models of sloshing for use in attitude control stability and control analyses. Understanding low-g slosh dynamics is especially needed for spacecraft with very large propellant mass fractions; of which there appear to be many in future space exploration architectures. It should be noted that typically the propellant motion in the low-g slosh regime is more complex to analyze than the high-g propellant motion. One key difference from the high-g slosh behavior is that the liquid propellant free surface is highly curved, with a zero-degree contact angle, in the low-g regime [ref. 40, Section 2.1]. While the spring-mass and pendulum mechanical models can be applied to the low-g slosh problem they may require the inclusion of some correction terms obtained from CFD simulation. Lastly, for completeness and as shown in Appendix G, there is a micro-gravity slosh regime (Bo < ~30) as well. Obviously the GN&C analyst should compute the Bond number that pertains to their specific slosh dynamics problem.

References 11, 25, 26, 27, and 44, all from Section 2.1, provide additional material on liquid propellant slosh dynamics covering topics from simplified slosh modeling techniques to discussion of the treatment of slosh stability margin reductions for human-rated launch vehicles.

Summary:

In closing, it should be emphasized that the stability of a feedback control system is its most intrinsic property. Simply satisfying performance requirements without ensuring stability in the face of uncertainty is not an acceptable design practice. Stability comes first, followed only then by performance. To gain a further appreciation of this fundamental fact readers are directed to Reference 43 by Gunter Stein, which was the first Hendrik W. Bode Lecture given at the IEEE Conference on Decision and Control in Tampa, Florida, in December 1989. In this lecture, Stein focused on the consequences of instability in mission critical control systems and emphasized that the underlying physical principles of stability must be clearly understood by all control system engineers.

Mission and/or Lesson Learned Linkages:

- Appendix A: X-43, Mariner 10
- Aerospace LL #2, 27, 33
- GSFC GOLD Rule #1.30
- NASA LLIS #0400
- References (Section 2.2): 40-57
- References (Section 2.1): 11, 25-27, 36-44, 47

Relevant Questions:

1. How is data latency accounted for? Have all time delays in the control loop between sensor readout and actuation been accounted for in the analysis and simulation process?
2. Are different sample rates used in different segments of the control system? How are the effects of multi-rate sampling accounted for?
3. Are the sensor/actuator pairs collocated on the spacecraft or are they placed in a non-collocated manner on the spacecraft?
4. Has a specific written requirement been placed upon the minimum allowable first bending mode frequency of the spacecraft (including all its flexible appendages)?
5. Are any of the structural mode frequencies within a decade of the controller bandwidth in any mode of operation?
6. Are any of the structural mode frequencies within +/- 5% of the loop closure frequency in any of the controller modes? Was a specific "stay out" requirement imposed to ensure adequate separation between all spacecraft flexible mode frequencies and all control mode loop closure frequencies?
7. How was the initial validation of the structural model accomplished before the results were integrated into the controller linear model?
8. Have MUFs been used add conservatism to pre-launch predictions of flexible body dynamics, as represented in the FEM? If so, is there a well defined, established, and consistent MUF policy being used at the start of the CSI analysis process? Is there a well-defined approach for MUF "burndown" over time as the flight system hardware matures and the FEM has increasing modeling details and test correlations?What experimental data supports using a particular value of damping ratio for the structural flexible body analysis? What effect does temperature have on the structural flexible mode damping ratio?
9. What techniques were employed in the control system design process to reduce the complexity (high-order) of the spacecraft flexible body model? Has the control system analyst performed a rigorous modal significance analysis to identify and retain all flexible modes with significant modal amplitude between a given actuator-sensor pair, or has the flexible dynamic model been formed by simply truncating the modal data above a specified frequency?
10. How was the modal gain and modal frequency data from the structural model been integrated into the controller linear model?

11. Does the control system analyst understand all the implications of the structural coupling terms used to connect the spacecraft structural sub-elements in the structural model? What data consistency and unit checks were performed on the modal data by the control system analyst prior to performing any stability analysis?
12. Do the flexible body dynamic properties of the spacecraft change significantly over the duration of the mission either as a result of alterations in vehicle re-configurations, re-orientations of moveable appendages (e.g., the slewing of solar arrays or re-pointing of communications antennas) and/or the expenditure of on-board consumables such as propellant?
13. Have structural model modal data outputs been provided to the GN&C analysts for the full range of solar array, communications antenna, deployable boom/mast, or other appendage angles and motions? Has the analyst repeated the flexible body stability analysis for all spacecraft core body/appendage configurations?
14. Was the frequency and the amplitude of all flexible modes varied in the course of performing the stability analysis? What was the range of variation used? Were all modes varied simultaneously in the analysis?
15. If digital "bending mode" filters (e.g., a low pass filter, a notch filter, etc.) will be utilized in the control loop to attenuate flexible body responses, has the frequency response analysis taken into account the execution rate? During flight, if it is necessary to adjust the frequency response characteristics of a digital "bending mode" filter will it be possible to update filter coefficients (and the filter initialization parameters) with only simple changes to FSW data tables or will such adjustments require FSW code patching?
16. What factors were considered, and what trades were performed, in selecting the sample rates for the feedback controllers used in each mode of spacecraft operation? In designing the spacecraft's sampled data feedback controller what protections were included to guard against the phenomena of aliasing introduced by under-sampling? Are anti-aliasing filters included as part of the controller design?
17. Have Monte Carlo techniques been used to perform stability analyses by simultaneously randomizing the bending mode frequencies, modal gains, damping ratios, and other parameters that effect stability?
18. Has a comparison been performed between the stability robustness values obtained from the linear frequency domain analyses and those obtained from the non-linear time domain simulation? How are the stability margins determined in the non-linear time domain simulation?
19. How are the stability margins determined in the HITL tests?
20. Are the natural frequencies derived by structural analysis confirmed through modal testing? What spacecraft-level, subsystem-level or component-level tests have been performed to validate the structural model?
21. Were any persistent small amplitude oscillations observed in either the closed-loop test data or the high fidelity simulation? Has the oscillation source been identified and corrective action been taken?

22. Have describing functions been used to study the influence of nonlinearities on control system stability? Does the describing function analysis predict the possibility of limit cycles?
23. If the control system has multiple inputs and multiple outputs, how were the stability margins determined?
24. Does the mission require relatively large amounts of propellant for orbital insertion, orbital manuevering, and/or reaction wheel momentum unloading such that a slosh dynamics analysis should be performed? Specifically, what is the ratio of the liquid propellant mass to the spacecraft dry mass at the start of the mission? Is this ratio in the range of 20% - 30% or greater?
25. Has the Bond number been calculated for the specific slosh dynamics problem under consideration? If so, does the Bond number indicate a high-g slosh regime or a low-g slosh regime?
26. Is there anything novel or unique about the size, shape, location, and configuration of the propellant tanks on the spacecraft?
27. Do the liquid propellant tanks have bare walls, internal diaphragms or bladders, other forms of PMDs, or anti-slosh baffles? If there are features internal to the propellant tanks, how has that influenced the determination of the slosh mode damping values?
28. Was a computational fluid dynamics (CFD) model used to support the formulation of the slosh model?
29. Has slosh ground testing been conducted using flight-like tanks to support the development of slosh dynamics models?
30. How have the liquid propellant slosh dynamics been modeled for the purposes of performing an attitude control system stability analysis? Was some form of mechanical slosh model developed to represent the vehicle's slosh dynamics? If so, which mechanical model was used: spring-mass or pendulum? Were any CFD-derived correction terms applied to the mechanical model to account for complex liquid propellant motions?
31. What specific value (or range of values) for the open-loop slosh mode damping ratios were used in the attitude control system stability anaysis?
32. Was the slosh model used for the stability analysis parameterized as a function of the propellant tank fill fraction and spacecraft linear acceleration?
33. Is the degree of dynamic coupling between the liquid propellant slosh modes and the spacecraft's flexible body modes well undestood?
34. How was the slosh model integrated into the attitude controller linear model?
35. What is the impact of liquid propellant slosh modes on the atttitude control system stability margins? What range of slosh model parameter variations was used to investigate the impact of slosh on attitude control system stability?
36. Have targeted sensitivity studies been conducted in the frequency and time domains to analyze and investigate the effects of slosh parameter and other system variations?

GN&C Best Practice #13

Ensure the analyses of the dynamics in ALL flight phases are understood completely (e.g., aerodynamics, flexibility, damping, gyrodynamics, plume impingement, moving mechanical assemblies, fluid motion, changes in mass properties, thermal snap).

Discussion:

Satisfactory dynamic performance of spacecraft ultimately depends upon accurate stability and control analyses. Often, sophisticated models of the dynamics of the spacecraft, its control system, and the environment are required to perform the required analyses. The first step in planning the analysis and simulation campaign is to identify how precise the models need to be for the pertinent vehicle dynamics and environments (e.g., aerodynamics, magnetic interactions, flexibility, damping, gyrodynamics, plume impingement, moving mechanical assemblies, fluid motion, changes in mass properties). Appropriate planning requires early consultation with dynamics and controls engineers who have broad experience on many missions and detailed experience on the specific types of problems that the current mission might encounter.

During the planning phase, preliminary analysis is required to estimate the magnitude of the environmental disturbances in order to size the control actuators and momentum storage devices appropriately. The disturbance environment may differ by many orders of magnitude over the different phases of a mission. Never the less it is usually "paper and pencil" analysis that is needed in the early stages of a program rather than computer simulation. The preliminary analysis is often more critical for systems that seem to be the simplest from a control systems point of view. The dynamics of space vehicles that are stabilized by gravity gradient, spinning, or momentum bias can be highly complex and inappropriate model simplifications such as linearization can lead to unstable designs. Non-linearities and cross-coupling between axes need to be treated with care starting with the preliminary analysis, because these phenomena are inherent in the physics; they are not necessarily second order effects that can be added as refinements later. It would be even more dangerous if the detailed performance analysis models used the same simplified assumptions as in a cursory preliminary analysis.

Three-axis stabilized spacecraft with sophisticated attitude determination and control systems may present analytical complications due to non-rigid body dynamics. Prior experience on similar spacecraft usually provides a reasonable basis for estimating how extensive the dynamics analysis and simulation campaign will need to be. Preliminary analysis for three-axis stabilized spacecraft is more likely to be required for unique control system design issues such as controller non-linearities, noise, and timing rather than unknown vehicle dynamics. Spin-stabilized spacecraft often present analytical complications due to energy dissipation, inertia ratio stability constraints, deployment uncertainties, fuel migration and thermally induced asymmetries.

Preflight predictions of the performance of GN&C systems are based on simulation because it is so difficult to replicate the space environment in a ground test facility. A Monte Carlo simulation campaign is often used due to the large number of variable parameters (e.g., atmospheric density, gyroscope noise, thruster valve response times, GPS receiver noise, modal frequencies, damping ratios) represented in the simulated dynamic model. The Monte Carlo campaign calculates multiple scenarios of a model by repeatedly sampling values from the probability distributions for the uncertain variables and using those values in individual simulations. A probabilistic

estimate of control system performance can then be calculated by taking an average over a large number of the random individual cases. Approximate formulae may be used to estimate how many cases will be required to achieve a specified confidence that the performance will be within a certain percentage of the goal; for complex systems that number of cases is often in the thousands. However, the campaign should be continued until the first two statistical moments (i.e., average and standard deviation) over the number of runs approaches a steady state and familiar distribution curves start to emerge that do not change significantly with additional cases.

The Monte Carlo simulation approach is a powerful tool that can be applied to a number of GN&C-related problems. For example, it has been used effectively to assess and understand the performance of spacecraft attitude determination and control systems, launch vehicle powered guidance systems, powered descent planetary landing systems, and space navigation systems. One other common and very useful application of the Monte Carlo technique is the evaluation of control system stability robustness.

Mission and/or Lesson Learned Linkages:

- Appendix A: Explorer 1, Lewis
- Aerospace LL #27, 95
- GSFC GOLD Rules #1.30, #1.31
- NASA LLIS #0400, 0423, 0424, 0625, 1480

Relevant Questions:

1. If the mission has a spinning phase, is the system stable over the range of inertias expected? If it is a dual-spin vehicle, does the effective inertia ratio pass through unity during despin?
2. What possible sources of energy dissipation exist? What damping time constant would be associated with them?
3. Does the selected GN&C architecture, or operational phases, levy inertia ration constraints on the system (or vice versa)?
4. Are linear control actuators required or will simpler bang-bang control suffice?
5. What is the tradeoff in control system bandwidth between sensor noise and disturbance torque?
6. What sampling rate is required for digital controllers? How much delay is permissible?
7. Is there a documented description of the simulation campaign used to predict GN&C performance and stability?
8. If the campaign involved Monte Carlo simulation, how many random variables were involved, what distributions for them were assumed, and how was the required number of cases (runs) determined?
9. Describe the process for establishing and validating the model uncertainties.

GN&C Best Practice #14

Make certain that the analyst who develops the mathematical models for the simulation of the GN&C hardware has hands-on familiarity with the hardware being modeled. All unexpected results or anomalies during hardware testing must be explained and/or incorporated into the simulation math model. Similarly, all deviations between results from the design simulation and the V&V simulation must be explained.

Discussion:

Skylab, like all space vehicles, was built with careful control of access to keep the vehicle clean, inventory all material brought inside, and prevent interference with the assembly and checkout crews. As a result, the designers rarely viewed their final product in the as-built condition**.** Clean room restrictions inhibited the detail designers from examining the hardware, even though several independent reviews had expressed concern about the deployment of the micrometeoroid shield**.** At approximately 63 seconds into the flight of Skylab 1 on May 14, 1973, an anomaly resulted in the complete loss of the meteoroid shield around the orbital workshop. A design error resulted in premature deployment of the shield, nearly causing a total loss of the mission**.** This initial anomaly was followed by the loss of one of the two solar array systems on the workshop and a failure of the interstage adapter to separate from the S-II stage of the Saturn V launch vehicle. The ensuing failure investigation identified the most probable cause of this flight anomaly to be the breakup and loss of the meteoroid shield due to aerodynamic loads not accounted for in its design. The breakup of the meteoroid shield, in turn, broke the tie-downs that secured one of the solar array systems to the workshop. Complete loss of this solar array system occurred at 593 seconds, when the exhaust plume of the S-II stage retro-rockets impacted the partially deployed solar array system. Falling debris from the meteoroid shield also damaged the S-II interstage adapter ordnance system in such a manner as to preclude separation. An important Lesson Learned here was that access to assembly areas should be controlled but not eliminated to ensure that engineers become familiar with actual flight hardware to develop an intuitive understanding of their system modeling results [ref. 60].

GN&C systems analysis and simulation studies require detailed models of guidance and control components (i.e., sensors, electronics, and actuators). The models are developed from component specifications, circuit diagrams, and test results. In the case of sensors and actuators, the models are derived from manufacturer specifications and test results. Electronics models are developed by breadboarding and laboratory testing of circuits and components. Test plans and results need to be reviewed by the analyst who develops the model to make certain the models conform to the hardware as it is actually built. It is highly advisable to have the analyst who develops the math models for the GN&C simulations participate in all major hardware design reviews as well as witness the hardware acceptance testing and review all test data generated. This will ensure the analyst has a high level of familiarity with the idiosyncrasies and behaviors of the GN&C hardware being modeled. The analyst and the test engineer must identify and resolve all test discrepancies. The detection and identification of discrepancies during testing has proved to be crucial to mission success in the past.

GN&C designers must ensure that they have used adequate dynamic modeling of structural flexibility, plume impingement, outgassing, liquid propellant slosh, nutation, etc. The dynamics and environmental models used in the GN&C design simulations cannot be tested easily in the

laboratory. Instead, they are tested against the truth models that were independently derived by the V&V team. The environmental models used in the two simulations can be tested individually by turning off all other models of disturbance sources. Similarly, flexible body dynamics can be compared by turning on one flex mode at a time for model validation. In general, the simulation test results will not match perfectly because the models were developed separately. However, the sources of the mismatch should be identified. If the mismatch is due to lack of completeness of the design simulation model, then it may need to be modified to provide higher fidelity, which in turn may result in retuning the GN&C system parameters.

Mission and/or Lesson Learned Linkages:

- Appendix A: ACRIM, TIMED, Terriers
- Aerospace LL # 2, 36
- NASA LLIS # 0377, 0641

Relevant Questions:

1. Was the analyst who developed the mathematical model of the component present when the hardware test was conducted?
2. Are all the idiosyncrasies and behaviors of the GN&C hardware, for all relevant mission phases, well understood?
3. Was the math model of the component used to predict expected test results? How well did the test results correlate with the expected values?
4. Were discrepancies between test results and expected values due only to parameter variations? Are the parameter variations consistent with the specified tolerances from the component manufacturer?
5. Is the GN&C closed-loop system performance sensitive to variations in actuator parameters such as stiction or backlash?
6. Were the physical parameters used in the dynamics and environmental math models based on experimental data? What range of values might be encountered in space during the mission?
7. What are the computational cell size dimensions used in the math models for pressure forces such as aerodynamics and solar radiation pressure? Is shadowing included in the models?

GN&C Best Practice #15

The truth model used in verification of high-fidelity simulations must be developed independently from that used in the design simulation.

Discussion:

Spacecraft contractors have the primary responsibility for performing sufficient stability, control, and dynamics analyses to assure satisfactory dynamic performance of the vehicle. These analyses need to be validated by an independent group in order to assure their completeness and correctness. The formulation of the math models used for verification should be independently derived from those used by the GN&C design engineers. Modeling mistakes are not easily caught. Reusing a model without fully understanding underlying assumptions can be risky. Changes in configuration or flight environment may invalidate the original analysis.

Programs should insist that the analysts document their methodology and assumptions, and compare them against the actual hardware so that errors may be found. Analysis does not negate testing. Component test plans and results must be reviewed to make certain that the models conform to the hardware as it is actually built. Designers should be called back to inspect the products, to see if there are major differences between analysis and implementation.

Mission and/or Lesson Learned Linkages:

- Appendix A: Explorer 1, IMAGE, Polar BEAR, Lewis, Voyager
- Aerospace LL #2, 38, 73
- NASA LLIS #0377, 0400, 0423, 0424, 0625, 0641, 1480

Relevant Questions:

1. If a model has been reused, did the original analyst review the model's applicability for this reuse?
2. Are the physical parameters (e.g., mass properties, gains, deadbands, aerodynamic density) that were used in the design simulations the same as in the verification simulation?
3. How were the math models of the components correlated with H/W test data?
4. Are all relevant dynamics modeled (e.g., nutation, multi-body dynamics, relative motion, flexibility, energy dissipation, fluid motion, magnetics, radiation pressure, aerodynamics, eddy current damping, out gassing, impingement)?
5. Are the simplifying assumptions used in formulating the model (e.g., small angle approximations, linearity, absence of cross coupling) justified over the entire range of conditions that the model will be used?
6. Has the fault protection logic been independently verified?

GN&C Best Practice #16

Establish a strong relationship with, and maintain close surveillance of, the GN&C lower-tier component-level (both hardware and software) suppliers.

Discussion:

The Apollo Program placed an extraordinary emphasis on GN&C component reliability. It was a single-string system with no redundant features, and thus, no fault tolerance. To achieve this unprecedented level of component reliability, a set of extremely rigid and comprehensive quality control processes were developed and applied by NASA on all Apollo GN&C parts and components suppliers. To satisfy the Apollo Program's need for an ultra-reliable GN&C system some industrial contractors established special NASA-dedicated Apollo Program production lines, using NASA certified trained assemblers. NASA personnel continuously performed on-site inspections of the Apollo GN&C component production lines at selected industrial contractors. At the electronic device level, all Apollo devices were tested and if a single sample proved defective the entire device lot was quarantined. Failed devices went through detailed teardown and failure analysis to preclude defect migration problems. Extensive component-level testing, including stress testing, was performed as part of the Apollo Program.

Following Apollo, NASA purposefully moved away from a single-string GN&C architectural approach for its human rated spacecraft. The GN&C systems implemented on the Shuttle Orbiter and the ISS have varying degrees of fault tolerance. Having fault tolerant spacecraft GN&C systems does not mean however, that NASA has the luxury of relaxing requirements for GN&C component-level reliability. NASA's industry partners (e.g., spacecraft system integration prime contractors) will have the leadership role in procuring GN&C components for their respective vehicles from the lower-tier suppliers. However, it would be inappropriate, unwise, and complacent for NASA to relinquish to the industry primes the entire responsibility for monitoring and overseeing the component development and production work at the suppliers.

NASA should share responsibility with the industrial prime contractors for shaping suppliers' technical, mission assurance, and business environments. In the past, NASA's concerns over interfering with the contractual relationship in place between the prime and a supplier encouraged an arms-length approach to suppliers by NASA project managers and engineers alike. In the future, NASA needs to find creative ways to be more proactive and involved with the selection of and contractual relationship formulated with the GN&C suppliers. NASA project managers should strongly encourage the primes to 1) select high-performing suppliers at all tiers of the supply chain; 2) effectively integrate NASA engineering and mission assurance teams into the prime-supplier relationships; and 3) ensure that best supplier practices for technical, mission assurance, and business processes are put in place at all tiers of the supply chain. For example, NASA should consider the potential benefits to be gained by putting in place contracts that offer long-term benefits (e.g., financial incentives) to both the prime and the suppliers for satisfactory (e.g., failure and malfunction free) on-orbit component-level mission performance. By jointly fostering a collaborative environment between NASA, the industry primes, and all tiers of suppliers, the likelihood of NASA achieving its primary objectives of crew safety and mission success will be increased.

Comprehensive design verification through the application of a rigorous test program starts with component-level testing at the suppliers. Emphasis needs to be placed upon the testing done at the lowest level under flight-like conditions. A strong on-site presence to closely monitor the planning, execution, and results of these component-level tests would have great value. The premise here is that an on-site engineer could identify problems/issues early enough to increase the probability of a timely and efficient resolution.

Obviously, having consistent manufacturing process controls as well as following the traditional standard approach for sequential developmental, qualification, and acceptance testing will directly support the goal of producing a known quality GN&C component at the supplier's facility. Unfortunately, it is not uncommon that programmatic cost and schedule pressures can arise due to the supplier encountering technical difficulties and unknown risks during component development. Note that the source of some of these pressures may also be traced to contractual provisions for award fees based upon the supplier's cost and schedule performance. The GN&C engineer must be aware of the buildup of these pressures and be poised to respond to their technically detrimental consequences. These consequences often will take the form of deliberate reactionary compromises in the design and qualification of components. Such compromises may materialize as 1) a push by the supplier towards component qualification by similarity; 2) limited, perhaps at the breadboard level only, developmental testing; 3) the premature release of component build drawing packages to the factory floor in parallel with, or perhaps even prior to, the completion of all developmental testing; 4) limited or constrained qualification testing; and 5) a reluctance to acknowledge design shortcomings, the need for re-design, and/or to perform any re-testing. Close routine on-site monitoring of suppliers' work will help identify any trends towards compromising component design and qualification integrity. Early recognition of such trends can be the key to successfully countering such technical compromises.

There is no substitute for regular face-to-face communication with the component supplier's design engineering, manufacturing, and test team members. Having a routine visible on-site presence at the supplier's facility on the part of the GN&C engineer establishes a pattern of technical ownership of the component, professional integrity, and attention to detail. In some special cases, it may be most beneficial to be physically co-located at the supplier's facility for some extended period, for example, during the qualification testing phase.

Establishing solid relationships with and maintaining close surveillance of GN&C hardware and software component suppliers is a best practice for human-rated and robotic spacecraft developments. However, one would expect the level of GN&C supplier surveillance to be substantially higher when procuring components for human-rated versus robotic spacecraft.

As part of the overall approach to monitoring the work of the component suppliers, the lead GN&C engineer should enlist the support, on an as-needed basis, of engineers, technicians, scientists, and statisticians with highly specialized education, training, skills and experience in such esoteric areas as software design and test, EEE parts, mechanical stress/loads, FMECA, electrical packaging, electromagnetic compatibility/interference (EMC/EMI), thermal design, mechanisms, reliability, manufacturing, tribology, environmental testing, software configuration management, ground/flight operations, and maintainability. For example, the GN&C engineer may call upon specialists to predict failure mechanisms and failure rates as well as specialists to make recommendations concerning life testing for components with moving parts such as

gyroscopes, CMGs, reaction wheel assemblies (RWAs), scanning Earth Sensors, antenna pointing mechanisms, etc.

Reference 34 highlights the effective combination of design, test and product assurance approaches used to achieve the high level of mission reliability required for the Apollo Program. On Apollo, at least half of the developmental failures that occurred in all the test programs were classified as due to workmanship, procedural, or quality causes. Over time, the Apollo design engineers and product assurance staff first learned how to screen out failures using high-reliability part-level process controls and quality inspections as well as component-level test techniques. The emphasis then was placed on preventing failures through design process improvements and, in tandem, identifying ways to catch failures earlier in the overall DDT&E process. Eventually, an area of primary concern and concentration for Apollo product assurance managers was to develop ways to reduce the number of failures that were "human-oriented" rather than "design-oriented." The author of reference 34 states that on Apollo, the probability of catching a "design error" in a spacecraft component was a function of the past test history of that component. In other words, the more successive tests, the greater the likelihood of the failure showing up. The author also states their probability of catching a "human error" was independent of the component's previous test history. This is because human-induced errors appeared in some units and not others, so the problem was different in a statistical sense.

The solution approach adopted by Apollo product assurance managers was to minimize the chances of inducing human errors (e.g., poor workmanship) and to place inspection and defect screening points around those areas where such errors would have the greatest probability of occurrence. Their goal was to catch these errors prior to subsystem ATP, and they focused on three distinct design aspects: design for producibility, design for rework and design for long equipment lifetime [ref. 34]. The value of the LM component pre-installation tests (PITs) performed by Grumman at their Bethpage assembly facility was also highlighted in reference 34. These PITs were performed on all components delivered to Grumman by their vendors as a protection against defects that may have passed through the vendor's pre-ship screens/tests or been induced during handling and transportation of the component. References 35–37 reinforce the points made on Apollo reliability by the author of reference 34. In particular, reference 35 describes the qualification and testing procedures used for the Apollo spacecraft components and systems with a special emphasis on vibration testing. Reference 37 gives a description of the reliability controls in U.S. crewed spacecraft programs up to the time of its publication (1974). This treatment covers Project Mercury, the Gemini Program, the Apollo Program, the Skylab Program, and the Apollo-Soyuz Test Project. Reference 37 summarizes the major reliability tasks and innovations being used on the Space Shuttle Program. Examples of these innovations include improved management techniques and an early identification of specific certification tests.

Mission and/or Lesson Learned Linkages:

References 34–37

Relevant Questions:

1. What process and criteria did the prime contractor employ to select the GN&C component suppliers? Was there a multi-stage down-select process?

2. Was the component design selected on the basis of lowest cost to just meet the minimum technical requirements and standards specified in the Request for Proposal (RFP)? Could a substantial improvement in component performance and reliability, beyond the minimum specified requirements, be achieved with modest cost growth? Is there a reasonable balance between "requirements creep" and being "penny-wise, pound-foolish" here in the selection of the component?
3. What is the past-performance record of the supplier in proving similar GN&C components under similar contractual conditions? Has the supplier previously provided components for human rated spacecraft or other aerospace vehicles?
4. What steps has the supplier taken to strengthen their qualification and verification of parts, materials, and processes to satisfy human rated spacecraft requirements?
5. What mission assurance standards and requirements are being placed upon the GN&C hardware/software component suppliers by the prime contractor? How has the prime contractor certified the GN&C hardware/software component suppliers can properly satisfy these imposed standards and requirements?
6. How has the prime contractor reinforced the government's expectation for reliable GN&C components that meet the technical standards and specifications for human rated spacecraft?
7. Does the supplier's contract include provisions for mission-level performance based financial incentives rather than (or in addition to) award fees based upon production cost and delivery schedule metrics?
8. Are there any formal contractual provisions (between the component supplier and the prime contractor) that will limit/constrain the government's access to the supplier's facility for general oversight and surveillance functions and, in particular, test witnessing?
9. What are the component-level test philosophies, criteria and implementation approaches being used by the suppliers? What specific aspects and features of the supplier's test program are intended to detect/screen out material, part, fabrication process, workmanship, and assembly defects in each component?
10. Does the component supplier have an adequate sized workforce with the right mix of design, manufacturing, and test engineering skills and experience?
11. What is the supplier's approach for the reporting, tracking and resolution of test discrepancies and anomalies? How will component "idiosyncrasies" found during testing be treated?
12. Does the supplier possess in-house all the required test facilities needed to conduct the entire component test program or are portions of the test program sub-contracted to other parties?
13. Does the prime contractor plan to co-locate engineering and mission assurance staff at the supplier's facility?
14. How well has the component supplier applied their lessons learned into own in-house design and development processes? What is the evidence of their success in doing this?
15. Are the technologies proposed by the supplier for a given component mature enough to proceed to the product development phase?

16. Which, if any, GN&C components does the supplier and the prime contractor intend to "Qualify by Similarity"? In each case what is the rationale for taking a qualification by similarity approach for a component?
17. Which GN&C components will require re-qualification because of obsolescence extensive changes in design, manufacturing and assembly processes, environmental levels and/or performance requirements?
18. Have the navigation sensors (particularly CCD-based optical sensors such as Star Trackers) been analyzed by the supplier for worst-case signal-to-noise degradations due to aging and exposure to the space radiation environment?
19. What approaches will the supplier use to ensure all testing is done in a safe manner to protect both flight hardware components and test team personnel?
20. Will an engineering or development model of the component be used as a "pathfinder" for validating test procedures prior to first application to flight hardware?
21. How will the component initial power-on test (IPT) procedures be validated prior to first use? How is safety ensured during such IPTs? How are components protected/safeguarded during IPTs?
22. Are there any special test fixtures or special test equipment not yet identified, costed, and scheduled?
23. Will GN&C component-level thermal/vacuum testing be performed in addition to ambient-pressure thermal cycling testing?
24. What component-level life testing is planned to be performed at the supplier's facility? What component-level life testing is planned to be performed at the prime contractor's facility?
25. Does the supplier intend to perform any tests for "discovery"? If so, what is the justification/rationale for such tests?
26. Will there be sufficient supplier-controlled documentation retained to assure that any subsequent failure, anomaly, discrepancy investigation or analysis that may be required can identify the specific manufacturing and assembly processes used, parts and materials used, and testing performed on each delivered flight component?
27. How have the qualification and acceptance test levels for vibration, thermal/vacuum, EMI, etc. been established at the component level for the specific mission application?

GN&C Best Practice #17

Ensure the GN&C subsystem adheres to the "Test As You Fly" philosophy.

Discussion:

In the development of a V&V testing program, the GN&C SE should be guided by the "Test As You Fly; Fly As You Test" maxim. The "verification" shows that the system (hardware and software) satisfies the design requirements, whereas the "validation" demonstrates that the system actually performs as intended.

More so than other spacecraft subsystems, it can be difficult to "Test As You Fly" for GN&C systems, which are severely constrained by the 1-g ground test environment. The GN&C V&V process therefore places an extraordinary reliance upon modeling and simulation. These models and simulations need to be independently validated.

"Test As You Fly" is the preferred method of GN&C verification. When this type of testing is either not possible or not appropriate, other verification methods (such as analysis, simulation, inspection, and demonstration) may be used. When analyses and/or simulations are used, the analysis and simulation results need to be independently reviewed. When inspections are used, they must be performed on the final, as-built, ready-to-fly GN&C configuration. The GN&C engineer should create a Test As You Fly Exception List documenting specifically where this test philosophy is not adhered to, including a description of the accepted risk to mission success.

The GN&C FSW must undergo closed-loop validation running on whatever platform is to perform as the GN&C host computer. It must be tested with nominal, failed and degraded GN&C components, over the full range of mission profiles, flight dynamics, and spacecraft models. Some GN&C functions can be tested on the ground without going to extraordinary measures. End-to-end attitude controller polarity tests can be performed in a relatively straightforward manner for example. The key is that these type of test need to be performed with rigorous knowledge and control of the test configuration. All such tests should be performed in the actual flight configuration, including the flight electrical harnesses and final GN&C FSW builds.

In addition, one should be testing for verification, not for "discovery." The expected results of a given test should be established and documented by the GN&C analyst well in advance of the actual test execution. The expected GN&C test results should be reviewed and understood by the test team prior to performing that test.

Mission and/or Lesson Learned Linkages:

- Appendix A: Lewis, WIRE, MCO, MPL, Timed
- Test As You Fly, Fly As You Test, and Demonstrate Margin (Mars Polar Lander, 1998), NASA Lessons Learned Information System, LL # 1196, 24 January 2002, JPL, https://llis.nasa.gov/lesson/1196
- Aerospace LL #53, 60, 80, 97
- GSFC GOLD Rules #1.07, #1.33

Relevant Questions:

1. Assuming that ground testing of all possible system configurations cannot be performed, how will the spacecraft's GN&C end-to-end behavior, stability, and overall performance be verified in various system configurations prior to actual in-flight implementation?
2. Has a GN&C Test Plan been formulated? Does this plan specify the scope of all GN&C test activities, roles and responsibilities, methods to be used, facilities and venues, models, support equipment, and schedule. The GN&C Test Plan should also clearly define the level of subsystem retest required, if any, in response to design changes, new software deliveries, and GN&C anomalies found in test.
3. Has the contractor developed a list defining the minimum set of GN&C tests that must be completed prior to launch? What are the mandatory ("must-do") GN&C tests needed to validate compatibility with the mission environments, and to demonstrate functional capability to execute the mission? How will deviation(s), if any, from the project-approved GN&C minimum test set be handled? Before any such deviations are approved by the Project, will an assessment of the resulting risk be provided?
4. Is it clearly defined in the plan what GN&C functions, performance, interfaces, and interactions with other subsystems:
   - Can be tested on the ground?
   - Can be tested on the ground but will not be tested?
   - Cannot be tested on the ground due to the realities of physics?
5. For those GN&C tests that can be tested on the ground but will not be tested by the contractor (i.e., there is no plan or allocated resources for these tests), has a sufficient GN&C engineering rationale been defined and documented? Does this rationale include the impact to the GN&C (and mission) risk posture?
6. Have all GN&C testing limitations and uncertainties been considered, defined, and documented? Have they been factored into the overall GN&C (and mission) risk posture?
7. To what extent will the actual GN&C flight hardware units, not the non-flight Engineering Units, be employed in GN&C testing?
8. What provisions has the contractor made to implement and enforce the "Test As You Fly" approach to GN&C testing? For example, does the contractor plan to perform GN&C end-to-end (sensor to actuator) controller polarity testing in the most flight like configuration possible? If so, what specific steps will be taken to ensure this happens?
9. Will simulated on-orbit "day in the life" operation of the GN&C subsystem be performed under nominal and stressed conditions for all mission critical events? In what test environment will these be conducted: Ambient conditions, or under exposure to expected thermal/vacuum and vibration environments?
10. Have all exceptions to the "Test-As-You-Fly" maxim within the GN&C tests program been identified and documented, along with an assessment of the resulting GN&C (and mission) risk? Has a Test As You Fly Exception List been created to specifficaly document where this test philosphy has not been adhered to, including a description of the accepted risk to mission success.

11. Once a desired “Test As You Fly” test configuration has been defined and established, how will it be maintained? What provisions has the contractor made to rigorously control the GN&C test configurations before, during and immediately after (which is necessary for any post-test troubleshooting work) the execution of a given test?
12. Does the contractor recognize controlling the GN&C hardware/software interface is of critical importance for any GN&C testing? What evidence is there that configuration management steps will be enforced to maintain this test environment?
13. Does the GN&C testing require unique procedures, special test equipment, GSE, test facilities and training for test personnel? Has the need for these items been documented in the GN&C Test Plan? Have sufficient resources (funding, personnel, and schedule) been allocated to ensure the timely phased delivery of the above to support the GN&C test team’s activities?
14. Does the contractor recognize and understand that the GN&C testing to be performed is for the purposes of verification, not for “discovery”? Have the expected results of a given test been clearly defined and documented by the GN&C analyst in advance of the actual test execution? Have these expected GN&C test results been reviewed and understood by the test team prior to performing that test?
15. Does the contractor plan to have a GN&C engineer that is knowledgeable of the requirements/test method and is independent of the test team “certify” the test procedures and the test configuration prior to use to ensure the planned testing represents an adequate GN&C verification step?
16. Does the contractor plan to us the same GN&C command/telemetry system for Flight Operations as was used for testing during the integration and test (I&T) phase of development?
17. Has a GN&C Trending Plan been developed describing how key component functional and performance metrics are to be tracked both during ground test and on-orbit?
18. Is there a plan to build an on-orbit GN&C hardware and software performance trend database upon similar trend data collected during the I&T phase? Have steps been taken to ensure that the I&T GN&C trend database is compatible with the on-orbit GN&C trend database so that they can be seamlessly integrated?
19. What GN&C testing can be performed at the fully integrated spacecraft level prior to shipment to the launch processing facility at the launch site? What are the specific limitations to GN&C testing at this point in the spacecraft development?
20. What GN&C testing can be performed at the launch processing facility? What are the specific limitations to GN&C testing at this point in the spacecraft pre-launch processing?
21. What GN&C testing can be performed on the launch pad? What are the specific limitations to GN&C testing at this point in the spacecraft launch configuration?
22. If the fully tested flight ready GN&C subsystem hardware/software configuration is altered what is the contractor’s approach for re-test?

23. When in the spacecraft DDT&E process will be the last test opportunity to ensure the GN&C subsystem will perform its intended functions?
24. Are non-operational demonstration spacecraft test flights planned to fill gaps in ground test capabilities and reduce risk to the future operational missions?
25. If no demonstration test flights are planned, are there early on-orbit tests that can be performed to fill gaps in ground testing before proceeding into the spacecraft's operation phases?
26. Has the contractor developed, prior to launch, a list that defines the minimum set of on-orbit GN&C tests that must successfully be completed prior to a given mission critical event in order to validate on-orbit readiness to perform that mission critical event (e.g., the successful accomplishment of inertial sensor calibrations and alignments prior to the trans-lunar injection burn)?
27. Have the GN&C FSW maintenance procedures, including real-time code patches, been demonstrated using flight-like communications links?

GN&C Best Practice #18

Plan and conduct true end-to-end sensors-to-actuators polarity tests in all flight hardware/ software configurations, including all flight harnesses/data paths, consistent with the "Test As You Fly" philosophy. Resolve all test anomalies.

Discussion:

Spacecraft use many GN&C components that can be easily reversed during installation. There have been many serious on-orbit problems, some leading to total mission failure, due to inadequate verification of signal phasing or polarity. Both component-level and end-to-end phasing tests are necessary to ensure correct operation. All GN&C sensors and actuators must undergo end-to-end phasing/polarity testing after spacecraft integration. The tests must be conducted using the same physical configuration and operational modes that will be used in flight.

Mission and/or Lesson Learned Linkages:

- Appendix A: TIMED, Terriers
- Aerospace LL #53, 97
- GSFC GOLD Rules #1.07, #1.33
- NASA LLIS #0194, 0281, 0288, 0310, 0345, 0383, 0390, 0403, 0726, 1370

Relevant Questions:

1. Do the photographs of the sensors and actuators show that they are mounted in the same positions and orientations with respect to the spacecraft coordinate frame during polarity tests as they will be in flight?
2. Is reorientation due to deployment properly taken into account for any of the GN&C components that are mounted on deployable structures such as solar arrays?
3. Were any special non-flight test cables or data paths used in the ground tests?
4. Were the tests conducted in all GN&C operating modes that will be used in flight? Was the operation of all switches and/or relays properly accounted for?
5. Did the test plan include a detailed list of the expected results? Were all deviations from the expected results thoroughly investigated and accounted for?
6. If any modifications were made either to the equipment or operational procedures as a result of the test are they properly documented? Were the tests that had been performed prior to the modifications repeated, or were they simply reviewed? How are configuration changes tracked?
7. Are there provisions in the FSW code and/or database to correct any polarity problems that might show up on orbit?

GN&C Best Practice #19

Plan and conduct sufficient GN&C HITL testing to verify proper and expected hardware and software interactions in all operational modes, during mode transitions, and in all mission-critical events.

Discussion:

The handover of control between redundant components or entire control systems, such as when mode switches occur, must be unambiguous. It may be desired to use the information about the end states of one control configuration as inputs for the initial states of the new configuration. However, once the handover is enabled, the new configuration must be completely in control and the former configuration must have no further effect on control. Conflict between control configurations can result in loss of control. All handovers must be tested in the flight configuration of the hardware and software to verify that the handovers are unambiguous.

In the past, engineering models for hardware and software test verification proved extremely valuable in closing the simulation/analysis loop.

Mission and/or Lesson Learned Linkages:

- Appendix A: Mars Polar Lander, Clementine, DART
- Aerospace LL #36, 53, 86

Relevant Questions:

1. Does the control system design rigorously control configuration, especially at hardware/software interface? Can glitches in one unit propagate across interfaces?
2. Were all flight-critical software functions tested with flight cables and data system HITL?
3. Does the test plan include both nominal and anomalous operational scenarios? Are all credible failure paths (e.g., part transients, latch-up, over-voltage, and EMI) included?
4. Did the tests include realistic switching to ensure a fail-safe transfer between redundant components and/or controllers?
5. Are there test points or software code embedded in the design that are used only during test? How are they disabled for flight?
6. Have non-flight engineering units (EUs) (also referred to as engineering models or EMs) of the GN&C hardware elements been procured to support GN&C HITL testing?
7. To what extent will the actual GN&C flight hardware units be employed in HITL testing?
8. Has the cost/benefit analysis of using the GN&C flight hardware units versus procuring EUs/EMs been performed? Specifically, has the risk of potentially damaging the flight hardware units during HITL testing been assessed and factored into the HITL planning?
9. If EUs/EMs will be used for testing, how will configuration control between flight and test units be managed?
10. How will GN&C design idiosyncrasies found during HITL testing be documented and addressed? How will the information on GN&C design idiosyncrasies be provided to the

design team, the ground operations team and the crew who will perform the flight operations?

11. Do the GN&C test planners understand the importance of creating and executing multiple off-nominal HITL test cases to rigorously stress the integrated hardware/software GN&C system in anomalous and contingency mission scenarios?

GN&C Best Practice #20

Treat GN&C ground databases, uploads, ground application tools, command scripts/files, etc., with the same rigor and disciplined care used for the GN&C FSW code and data.

Discussion:

The engineers who initially conceive and design a GN&C system often do not stay with the program through its entire life cycle. Consequently, the reasons behind the selection of certain parameters or operational procedures may not be apparent to spacecraft operators at a later time. Ad hoc changes in the databases or operational procedures can be fatal to the mission. Thorough training and adherence to the established procedures for ground software/database configuration management, documenting change history, version archiving, and peer review is essential for the flight operations team.

Mission and/or Lesson Learned Linkages:

- Appendix A: RME, GFO
- Aerospace LL #3, 29, 43

Relevant Questions:

1. Are command scripts formally controlled?
2. What is the procedure for establishing yellow caution and red alarm telemetry monitor limits? Is there an independent analysis of the values before flight?
3. What is the process to make changes in the databases?
4. Will the same GN&C command and telemetry system be used in I&T and for flight operations?
5. Under what operational circumstances must a GN&C system design engineer be notified?
6. Is there a document describing the type and extent of GN&C training that is provided to the flight operations team?
7. Does the GN&C System Design document explain in detail the rationale for the selection of ACS parameters and operations procedures?

GN&C Best Practice #21

Ensure that sufficient GN&C engineering telemetry data are down-linked to diagnose and resolve anomalies, particularly during all mission-critical phases, including the early on-orbit operational period when so many failures occur.

Discussion:

Anomalies occur in even the best of systems. The most important factor in resolving them is getting access to the right telemetry data. Having good data greatly simplifies diagnosis of the root cause of the anomaly and reduces the time required to correct it. The routine engineering telemetry that is available for evaluating normal operations is often inadequate to help resolve anomalies efficiently. Good diagnostic data typically includes many more variables and it is sampled at a significantly higher rate. Plans for providing sufficient diagnostic telemetry should be included in the initial designs of the GN&C and telemetry systems.

It is highly advisable to develop a set of ground displays for the GN&C engineers working launch and/or mission operations that will allow problems to be identified and diagnosed quickly. Ensure a dedicated real-time GN&C simulator is developed to allow these GN&C engineers to realistically train and rehearse critical GN&C operations in the manner they expect during launch and/or mission operations.

Mission and/or Lesson Learned Linkages:

- Appendix A: WIRE, ACRIM, Lewis
- Aerospace LL #53, 67
- NASA LLIS #0625

Relevant Questions:

1. What plans are in place to continue to add to the GN&C hardware and software performance trend database that was collected during the I&T phase with similar on-orbit trend data?
2. How many variables are in the telemetry lists for normal engineering data and diagnostic data? How many spare data slots are available?
3. What are the sample rates for normal engineering data and diagnostic data?
4. What is the maximum angular velocity that the spacecraft might reach in the event of a worst-case anomaly? Is the data rate for the diagnostic telemetry high enough, and the data scaling appropriate, to unambiguously track the relevant parameters in that situation?
5. Is the diagnostic data taken and temporarily stored automatically or does high rate sampling have to be enabled by a command? How much diagnostic data can be stored on-board?
6. What is the adaptive capability of the spacecraft's telemetry system to capture non-routine GN&C engineering data in support of anomaly resolution? In particular, does the spacecraft's telemetry system provide capabilities for adding new GN&C telemetry points, collecting specific telemetry points (e.g., inertial sensor outputs) in a high data rate "dwell mode" manner, and to re-scale selected telemetry data points?

GN&C Best Practice #22

Adhere to a "Train as They Fly" philosophy—Ensure that a dedicated real-time GN&C simulator facility is developed and maintained to allow the crew to realistically train and rehearse GN&C operations in the manner that they expect to actually fly the spacecraft.

Discussion:

From the early phases of Project Mercury through the Gemini and Apollo Programs, flight simulators have been the key elements in the astronaut training programs. As the missions progressed in complexity, the sophistication, number, and variety of simulators employed for astronaut training were increased correspondingly.

As described in reference 39, it was necessary to evolve the fidelity of these crewed spacecraft flight simulators to meet the escalating demands in crew training requirements. A review of the historical record shows that the Apollo astronauts relied much more heavily on spacecraft simulators than did the Gemini crews. Three sets of these simulators were developed—two at Kennedy launch site in Florida and one at the Johnson Crewed Spacecraft Center in Houston—modeled after the flight versions of the CM and the LM. The simulators, constantly being changed to match the cabin layout of each individual spacecraft, were engineered to provide the crew with all the sights, sounds, and movements they would encounter in actual flight. The Apollo crews would require about 180 training hours in the CM simulator plus an additional 140 hours in the LM simulator. This represented about an 80% increase in simulator training time compared with what the astronauts on the early Gemini flights had required.

Reference 39 points out that several key factors emerged during the Apollo Program as critical and basic for providing adequate flight simulators for astronaut crew training. First among these are high-fidelity crew stations, especially in the area of GN&C flight controls and displays. Another was identified as the accurate simulation of the guidance computer and navigation systems. Others included complete visual display systems for simulated out-the-window scenes and certain moving-base simulators for high-fidelity training in particular portions of the missions. The significance of each of these factors for new programs will depend to a large degree on the mission objectives and requirements. One can unequivocally state however that these spacecraft flight simulators, incorporating significant GN&C attributes in their design and operations, will be vital in future CxP astronaut training.

Astronaut "hands-on" involvement in the design and development of the GN&C systems and associated flight simulators is a must. Intensive training in a real-time functional simulator not only trains the crew in the operational aspects of the GN&C system but it also permits the crew to feedback information that will enhance safety, operational efficiency, and mission success.

The Astronaut crews are the ultimate "stake holders" of the GN&C design. Too often, the designer implements a fully automatic implementation routinely used in uncrewed spacecraft. Astronaut interchange to define needed critical display monitoring, mode sequencing with intervention provisions, alternative procedures and abort provisions are extremely valuable. Current technology enables many operations to be implemented automatically and sequenced as nominally indicated in various mission phases. Methods to provide astronaut assessment of

satisfactory performance and means to implement work around provisions should be a design requirement.

In the Apollo Program, astronaut participation in both the CSM and LM implementation meetings identified architectural mode enhancements as well as display and other monitoring provisions. Use of mockups and realistic simulators enabled extensive crew training. Understanding and familiarity with the functionality and operation of the GN&C system proved invaluable in reestablishing operation of the system after a lightning strike during the Apollo 12 launch. Manual control provisions enabled the divert maneuver by Apollo 11 when the auto selected landing site was observed as being hazardous.

Participation in mock up reviews facilitates the human engineering process and enhances the design. Extensive real-time simulations were in place during Apollo and the Shuttle development and fielding. The Shuttle program included a Shuttle Avionics Integration Laboratory (SAIL) and Shuttle Motion Simulator (SMS) facility with real-time operation and cockpit set-up. The SMS is used primarily for training and the SAIL is an engineering simulation that is open to Astronaut participation.

The real-time spacecraft simulator would support GN&C/human interaction training for the crew in normal and contingency operations of the GN&C subsystem. The crew would be able to refine and practice GN&C operations and contingency procedures without using valuable spacecraft time. The spacecraft simulator could also be used to validate GN&C command/telemetry data flows between the spacecraft and the ground network.

The GN&C engineering models built into such a real-time simulator would also allow the Crew to have input into GN&C/human interaction at an early design phase.

The GN&C simulator can be also used to support on-orbit operations, especially to checkout and validate new GN&C contingency procedures. The ability to implement alternate operational procedures and tests proved to be life-saving for Apollo 13.

Mission and/or Lesson Learned Linkages:

Reference 39

Relevant Questions:

1. Does the contractor intend to develop a real-time spacecraft-training simulator?
2. Are there special GN&C crew training requirements/needs? How will they be satisfied?
3. What will be the fidelity of the GN&C subsystem in such a simulator?
4. What range of situations (nominal and off-nominal) was tested with crew in the loop to ensure the design was robust?
5. Have GN&C contingency procedures been developed using the flight simulators that exercise all aspects of the critical mission phases?
6. Based on simulator testing, what information is deemed essential to the crew’s real-time understanding of the state of the vehicle(s)?
7. What information is deemed essential to crew’s understanding of the state of the automation?
8. How were the control mechanisms (e.g., hand controllers, keyboards, etc) identified and chosen?

2.0 References

2.1 Additional Post-2007 References

1. Design, Development, Test, and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems, NASA Engineering and Safety Center Technical Report, Document RP-06-108, Volume I and Volume II, Version 1.0, 3 May 2007.
2. GN&C Engineering Best Practices for Human-Rated Spacecraft Systems, Cornelius J. Dennehy, Kenneth Lebsock, and John West, AIAA GN&C Conference and Exhibit, NESC Invited Session, AIAA Paper 2007-6336, Hilton Head, South Carolina, August 2007. (Also published as NASA TM-2008-215106, January 2008.)
3. Crew Safety Considerations, D.K. Slayton, International Astronautical Federation paper IAF-A-76-01, Anaheim, California, 10-16 October 1976.
4. Connecting Engineers to Online Experts and Knowledge, Neil Dennehy, Daria Topousis, and Kenneth Lebsock, NASA Project Management Challenge 2010, February 9-10, 2010, Galveston, TX.
5. System Architectural Considerations on Reliable Guidance, Navigation, and Control (GN&C) for Constellation Program (CxP) Spacecraft, Cornelius J. Dennehy, NASA TM-2010-216716 (also published as NESC Final Report RP-06-074), July 1, 2010.
6. The Value of Identifying and Recovering Lost GN&C Lessons Learned: Aeronautical, Spacecraft, and Launch Vehicle Examples, Cornelius J. Dennehy, Steven Labbe, and Kenneth L. Lebsock, AIAA GN&C Conference, NESC Invited Session, AIAA Paper 2010-8429, Toronto, Ontario, Canada, August 2-5, 2010.
7. Present Challenges, Critical Needs, and Future Technological Directions for NASA's GN&C Engineering Discipline, Cornelius J. Dennehy, 2010 AIAA GN&C Conference, NESC Invited Session, AIAA Paper 2010-8434, Toronto, Ontario, Canada, August 2-5, 2010.
8. Exploiting Online Expertise and Knowledge Sharing for the Benefit of NASA's GN&C Community of Practice, D. Topousis, C. J. Dennehy, and K. L. Lebsock, AIAA Guidance, Navigation, and Control Conference, NESC Invited Session, Toronto, Ontario, Canada, August 2-5, 2010.
9. Flight Anomaly Distillation Analyses Report 1995–2010, Joe Cavaluzzi, John Azzolini, and Michael Bay, December 30, 2010.
10. The Identification and Recovery of Lost Lessons Learned, Cornelius Dennehy and Kenneth Lebsock, NASA Project Management Challenge 2011, Long Beach, California, February 9-10, 2011.
11. Identification of Lessons Learned from the NESC's Orion-Ares Propellant Slosh Assessment, Supplement to NESC Final Report NASA/TM-2011-217183 (NESC-RP-09-00602, Version 2), N. Dennehy, February 11, 2011.
12. The Development of NASA's Fault Management Handbook, Lorraine Fesq, Neil Dennehy, et al, SAFEPROCESS 2012, Mexico City, Mexico, August 29, 2011.

13. Technical Challenges and Future Technology Needs for NASA's Guidance, Navigation, and Control Engineering Discipline, Cornelius J. Dennehy, 35th Annual AAS Guidance and Control Conference, AAS Paper 12-061, Breckenridge, Colorado, February 2012.

14. GN&C Engineering Lessons Learned from Human Space Flight Operations Experiences, Gary Dittemore and Cornelius Dennehy, Proceedings of the EuroGNC 2013, ThCT3.1, 2nd Council of European Aerospace Societies (CEAS) Specialist Conference on GN&C, Delft University of Technology, Delft, The Netherlands, April 10-12, 2013 (https://aerospace-europe.eu/media/books/delft-0058.pdf).

15. GN&C Engineering Discipline Lessons Learned from NASA's Experiences with Human Spaceflight Operations, Cornelius J. Dennehy and Gary D. Dittemore, AIAA Paper 2013-5321, AIAA SPACE 2013 Conference and Exposition, San Diego, California, September 10-12, 2013.

16. Designing for Flight Through Periods of Instability, Cornelius J. Dennehy, NESC Technical Bulletin No. 14-01, May 2013.

17. A Comprehensive Analysis of the X-15 Flight 3-65 Accident, Cornelius J. Dennehy, Jeb S. Orr, Immanuel Barshi, and Irving C. Statler, NASA/TM 2014-218538 (NESC-RP-14-00957), October 2014.

18. Guidance, Navigation & Control Lessons Learned from Spacecraft Relative Motion Missions, C.J. Dennehy and J. Russell Carpenter, WeA1 Tutorial Session: Spacecraft Relative Motion GN&C: Missions, Technology, & Theory, 2015 European Control Conference, Linz, Austria, July 15, 2015.

19. Transitioning to Highly Autonomous Systems: NASA Space Mission Perspectives, Cornelius J. Dennehy, Draper Autonomous GN&C Symposium, Cambridge, Massachusetts, November 4, 2016.

20. Some Perspectives on Piloted Spacecraft from a Guidance, Navigation, and Control (GN&C) Viewpoint, C.J. Dennehy, NESC 2016 Technical Update Article, November 2016.

21. Navigation Filter Best Practices, edited by J. Russell Carpenter and Christopher N. D'Souza, NASA TP 2018-219822, April 2018.

22. Guidance, Navigation and Control (GN&C) Lessons Learned and Associated Best Practices, Cornelius J. Dennehy, Invited Knowledge Management Presentation at ESA/ESTEC, Noordwijk, The Netherlands, June 6, 2017.

23. Navigation Filter Best Practices, Cornelius J. Dennehy, NASA Engineering & Safety Center Technical Bulletin No. 19-01, July 2019.

24. Verification and Validation (V&V) Challenges for Future Space Guidance, Navigation, & Control (GN&C) Systems: A Multi-Agency Workshop and Seminar Series, Seminar Series Kickoff Talk – ESA and NASA Perspectives, Samir Bennani and Cornelius J. Dennehy, September 15, 2020.

25. Treatment of Launch Vehicle Flight Control Stability Margin Reductions for Crewed Missions with Emphasis on Slosh Dynamics, NESC Best Practices Report, Neil Dennehy, Tannen VanZwieten, and John Wall, June 15, 2022.

26. NESC Technical Bulletin, 2022-05, “Launch Vehicle Flight Control Stability Margin Reduction Considerations,” August 2022.

27. NESC Technical Bulletin, 2022-06, “Treatment of Slosh Stability Margin Reductions for Human-Rated Launch Vehicles,” August 2022.

28. NESC GN&C TDT Best Practices: Design Requirements for Satisfactory Handling Qualities of a Piloted Spacecraft, NASA/TM−20220013375 (NESC-IB-22-05), John Osborn-Hoff, Cornelius J. Dennehy, and Cynthia H. Null, August 2022.

29. Recurring Causes of Human Spaceflight Mishaps during Flight Tests and Early Operations, NASA/TM-2020-220573 (NESC-RP-12-00823), Timothy S. Barth, et al, March 2020.

30. Spacecraft Micro-Vibration: A Survey of the Problems, Experiences, Potential Solutions, and Some Lessons Learned, Cornelius J. Dennehy and Oscar S. Alvarez-Salazar, European Conference on Spacecraft Structures, Materials & Environmental Testing (ECSSMET2018) May 28-June 1, 2018, ESA/ESTEC, The Netherlands, May 29, 2018.

31. Managing Observatory Line-of-Sight Jitter: A “Jitter 101” Process Overview, Gary J. Henderson, Aerospace Corporation, January 30, 2019.

32. A Survey of the Spacecraft Line-of-Sight Jitter Problem, Cornelius Dennehy and Oscar S. Alvarez-Salazar, AAS Paper 19-131, 42nd AAS Annual Guidance and Control Conference, Breckenridge, Colorado, February 1-6, 2019.

33. GOES I-M: A Retrospective Look at Image Navigation and Registration (INR), Jitter, and Lessons Learned, John Sudey, Jr., Michael Hagopian, and Cornelius Dennehy, AAS Paper 19-132, 42nd AAS Annual Guidance and Control Conference, Breckenridge, Colorado, February 1-6, 2019.

34. A Survey of Reaction Wheel Disturbance Modeling Approaches for Spacecraft Line-of-Sight Jitter Performance Analysis, Cornelius J. Dennehy, 18th European Space Mechanisms and Tribology Symposium (ESMATS), Munich, Germany, September 18-20, 2019.

35. Spacecraft Line-of-Sight Jitter Mitigation and Management Lessons Learned and Engineering Best Practices, Cornelius J. Dennehy, Aron Wolf, and Davin Swanson, 11th International ESA Virtual Conference on Guidance, Navigation & Control Systems, June 24, 2021.

36. Bauer, H.F., “Propellant Sloshing Problems of Saturn Test Flight SA-1,” NASA TM-X-50497, March 20, 1962.

37. Bauer, H. F., 1964, “Fluid Oscillations in the Containers of a Space Vehicle and Their Influence on Stability,” NASA TR R-187.

38. Ryan, R.S., “A History of Aerospace Problems, Their Solutions, Their Lessons,” NASA TP-3653, September 1996.

39. The Dynamic Behavior of Liquids in Moving Containers, NASA SP-106, 1966, Abramson, H.N.

40. The New “Dynamic Behavior of Liquids in Moving Containers,” Southwest Research Institute, San Antonio, TX, 2000, Dodge, Franklin T.

41. A CFD Approach to Modeling Spacecraft Fuel Slosh, Brandon Marsell, et al, 2013.

42. NASA. Slosh Suppression, NASA Space Vehicle Design Criteria Monograph, NASA SP-8031, May 1969.

43. The Effects of Propellant Slosh Dynamics on the Solar Dynamics Observatory, Paul Mason and Scott R. Starin, July 25, 2011.

44. Dynamics and Simulation of Flexible Rockets, Timothy Barrows and Jeb Orr, AcademicPress/ Elsevier, 2022.

45. Lessons Learned/Knowledge Sharing Letter, Mike Ryschkewitsch and Bryan O'Connor, February 19, 2009.

46. Test As You Fly, Fly As You Test, and Demonstrate Margin (Mars Polar Lander, 1998), NASA Lessons Learned Information System, LL # 1196, 24 January 2002, JPL, https://llis.nasa.gov/lesson/1196.

47. An Introduction to the Fundamentals of Control-Structure Interaction, Davin Swanson and Neil Dennehy, NESC Academy GN&C "Beyond the Textbook" Tutorial Lecture, 40th Annual AAS Guidance and Control Conference, Breckenridge, Colorado, January 30-February 4, 2015. Aso see NESC Academy Webcast, same title, March 15, 2017.

2.2 Original Report References

1. NASA Document TP-2508, "Problems Experienced and Envisioned for Dynamical Physical Systems," Robert S. Ryan, August 1985.

2. NASA Document TN D-8227, "Apollo Experience Report- Guidance and Control Systems: Primary Guidance, Navigation and Control System Development," M. D. Holley, et al, May 1976.

3. NASA Document SP-287, "What Made Apollo a Success," 1971 (available online at: http://history.nasa.gov/SP-287/sp287.htm).

4. "Apollo Spacecraft," AIAA Paper, George M. Low, AIAA 6th Annual Meeting and Technical Display, Anaheim, California, October 20-24, 1969.

5. MIT, Instrumentation Laboratory, "A Recoverable Interplanetary Space Probe" rpt. R-0235, 4 vols., July 1, 1959. Project report. (cited by NASA SP-4212 "On Mars: Exploration of the Red Planet. 1958-1978," http://history.nasa.gov/SP-4212/sources2.html).

6. Hal Laning, et al, Interplanetary Navigation System Study, Report R-273, MIT Instrumentation Laboratory, April 1960.

7. C. S. Draper, "Origins of Inertial Navigation," Journal of Guidance and Control, AIAA Paper 81-4238, October 1981.

8. "The History of Apollo On-Board Guidance, Navigation, and Control," David G. Hoag, International Space Hall of Fame Speech, Draper Laboratory Report P-357, September 1976.

9. NASA Document SP-504, *Shuttle Avionics Handbook*, John F. Hanaway and Robert W. Moorehead, Washington, D.C.: National Aeronautics and Space Administration, 1989.

10. NASA Document SP-2000-6109, International Space Station Evolution Data Book, Volume 1, Baseline Design, Rev. A, Catherine A. Jorgensen (Editor), October 2000.
11. NASA Document TD9072A, International Space Station Familiarization 21109, Mission Operations Directorate, Space Flight Training Division, July 31, 1998 (available online at: http://www1.jsc.nasa.gov/er/seh/td9702.pdf).
12. NASA Document TP-2006-213168, "Three Years of Global Positioning System Experience on International Space Station," Susan Gomez, August 2006.
13. NASA Document CR-2005-213693, "GPS Lessons Learned from the International Space Station, Space Shuttle and X-38," John L. Goodman, November 2005.
14. "Autonomous Rendezvous, Capture and In-Space Assembly: Past, Present and Future," AIAA Paper 2005-2523, Douglas Zimpfer, P. Kachmar, and S.Tuohy, January 30, 2005.
15. NASA Document TP-1998-208528, M.E. Polites, "An Assessment of the Technology of Automated Rendezvous and Capture in Space," July 1998.
16. NASA Document SP-2004-4503, Monographs in Aerospace History, Number 3, "APOLLO: A Retrospective Analysis," Page 13, Roger D. Launius, Reprinted July 2004.
17. "Summary of Gemini Rendezvous Experience," AIAA Paper 67-272, E. Lunney, Cocoa Beach, Florida, February 1967.
18. "Apollo Lunar Rendezvous," AIAA Journal of Spacecraft and Rockets, Vol. 7, No. 9, Kenneth A. Young and James D. Alexander, September 1970.
19. "History of Space Shuttle Rendezvous and Proximity Operations," John L. Goodman, Journal of Spacecraft and Rockets, Vol. 43, No. 5, September-October 2006.
20. "Laser-Based Relative Navigation and Guidance for Space Shuttle Proximity Operations," AAS Paper 03-014, Fred D. Clark, P. T. Spehar, J. Brazzel Jr., and H.D. Hinkel, 5 February 2003.
21. "Shuttle-Mir Stories" (available online at: http://spaceflight.nasa.gov/history/shuttle-mir/history/h-f-foale-collision.htm).
22. "Satellite G&C Anomaly Trends," Brent Robertson & Eric Stoneking, AAS Technical Paper 03-071, February 2003.
23. "The NEAR Guidance and Control System," Thomas E. Strickwerda, J. Courtney Ray, and David R. Haley, Johns Hopkins Applied Physics Laboratory Technical Digest, Volume 19, Number 2, 2005.
24. **"**The Near Discovery Mission: Lessons Learned," by R. H. Maurer and A. G. Santo, The Johns Hopkins University Applied Physics Laboratory.
25. "NEAR Mission Overview and Trajectory Design," Robert W. Farquhar, David W. Dunham, and Jim V. McAdams, AAS/AIAA Astrodynamics Conference, Halifax, Nova Scotia, August 14-17, 1995.
26. "Shuttle Orbit Flight Control Design Lessons: Direction for Space Station," Kenneth J. Cox and Philip D. Hattis, Proceedings of the IEEE, Vol. 75, No. 3, March 1987.

27. “A Successful Strategy for Satellite Development and Testing,” Bill Tosney and Steve Pavlica, Aerospace Corporation Crosslink publication, Fall 2005 (available online at: http://www.aero.org/publications/crosslink/fall2005/01.html).

28. NASA Document TM-74736, “Crewed Lunar-Landing through the use of Lunar-Orbit Rendezvous,” J. C. Houbolt, 1961.

29. “Architecture Generation for Moon-Mars Exploration Using an Executable Meta Language,” Willard L. Simmons, Benjamin H. Y. Koo, and Edward F. Crawley, AIAA Paper 2005-6726, AIAA Space 2005 Conference, Long Beach, California, August 2005.

30. “The Influence of Architecture in Engineering Systems,” An MIT Engineering Systems Monograph, Edward Crawley, et al, March 29, 2004.

31. “More Apollo Guidance Flexibility Sought,” Aviation Week & Space Technology, November 16, 1964.

32. NASA Document TN D-8227, “Apollo Experience Report- Abort Planning,” Charles T. Hyle, Charles E. Foggatt, and Bobbie D. Weber, May 1976.

33. “Tales from the Lunar Module Guidance Computer,” AAS Technical Paper 04-064, Don Eyles, February 6, 2004.

34. AIAA Technical Paper 72-247, “Product Assurance Program Planning—Some Lessons Learned from Apollo,” Gerald Sandler (Grumman Aerospace Corp.).

35. “Testing to Ensure Mission Success,” Simpkinson, S. H., March 1, 1970, Astronautics and Aeronautics, Vol. 8, P. 50-55 (also listed as NTRS Document ID: 19700047589 with NTRS Accession ID: 70A23705).

36. “Apollo Spacecraft Certification Test Program and Applications for Future Crewed Spacecraft,” Fitzgerald, P. E. and Levine, J. H., AIAA Technical Paper 1970-375, American Institute of Aeronautics And Astronautics, Test Effectiveness in the 70s Conference, Palo Alto, Calif., April 1-3, 1970.

37. “United States Crewed Spacecraft Reliability Experience,” Kleinknecht, K. S., and Levine, J. H., September 1, 1974, IAF PAPER 74-049, 25th; Amsterdam; International Astronautical Federation, International Astronautical Congress; Netherlands; Sept. 30, 1974-Oct. 5, 1974, Role in Space Conference, Cocoa Beach, Florida, March 27-28, 1972.

38. Ariane-5 Flight 501 Failure, ESA/CNES Inquiry Board Report, Prof. J. L. Lions (Chairman), July 19, 1996, Paris, France.

39. “Apollo Experience Report: Simulation of Crewed Space Flight for Crew Training,” NASA Technical Note, Woodling, C. H., Faber, Stanley, Van Bockel, John J., Olasky, Charles C., and Williams, Wayne K., March 1973, DTIC Accession Number: ADF630602.

40. “Effects of Structural Flexibility on Spacecraft Control Systems,” NASA Space Vehicle Design Criteria Monograph, NASA SP-8016, April 1969.

41. “Multivariable Gain and Phase Margin Analysis of a Fully Coupled Six-Degree-of-Freedom Guided Missile,” Jonathan R. Bar-on’ and Robert J. Adams, Proceedings of the 1999 IEEE

International Conference on Control Applications, Kohala Coast-Island of Hawaii, Hawaii, USA August 22-27, 1999.

42. "Implementation Challenges of Multivariable Control Systems: What They Did Not Teach You In School," Sanjay Garg, Lesson 9, NESC Academy Course, *Satellite Attitude Control Systems: Learning from the Past and Looking to the Future*, June 2006, available online at http://www.nescacademy.org.
43. "Respect the Unstable," Gunter Stein, IEEE Control Systems Magazine, August 2003, Pages 12-25.
44. "The Impact of Remote Manipulator Structural Dynamics on Shuttle On-Orbit Flight Control," Sargent, D.G., AIAA Technical Paper 84-1963, Guidance and Control Conference, Seattle, Washington, August 20-22, 1984, Technical Papers (A84-43401 21-63). New York, American Institute of Aeronautics and Astronautics, 1984, p. 674-680.
45. "Feedback Amplifier Design," H. W. Bode, Bell Systems Technical Journal, vol. 19, p. 42, 1940.
46. "Regeneration Theory," H. Nyquist, Bell Systems Technical Journal, 1932.
47. Theory of Servomechanisms, H. M. James, N.B. Nichols, and R.S. Phillips, New York: McGraw-Hill, M.I.T. Radiation Lab. Series, Vol. 25, 1947.
48. "Graphical Analysis of Control Systems," W. R. Evans, Trans. AIEE, vol. 67, pp. 547-551, 1948.
49. "On the Input-Output Stability of Time-Varying Nonlinear Feedback Systems, Part I: Conditions Derived Using Concepts of Loop Gain, Conicity, and Positivity," G. Zames, IEEE Trans. on Automatic Control, AC-11:228-238, April 1966.
50. *A Complex Variable Approach to the Analysis of Linear Multivariable Feedback Systems*, Postlethwaite, I. and A. G. J. MacFarlane, Berlin: Springer-Verlag, 1979.
51. "The Generalized Nyquist Stability Criterion and Multivariable Root Loci," A. G. J. MacFarlane and I. Postlethwaite, International Journal of Control, vol. 25, pp. 81-127, 1977.
52. *Computer-Aided Control System Design*, H. H. Rosenbrock, New York: Academic Press, 1974.
53. "Analysis of Feedback Systems with Structured Uncertainties," J. C. Doyle, Proc. IEE, 129:242-250, 1982.
54. "Multivariable Feedback Design: Concepts for a Classical/Modern Synthesis," J. Doyle and G. Stein, IEEE Trans. on Automatic Control, vol. AC-26, pp. 4-16, Feb. 1981.
55. "Gain and Phase Margin for Multiloop LQG Regulators," M. G. Safonov and M. Athans, IEEE Trans. on Automatic Control, AC-22 (2), 173-179, 1977.
56. "Feedback Properties of Multivariable Systems: The Role and Use of the Return Difference Matrix," M.G. Safonov, A. J. Laub, and G.L. Hartmann, IEEE Trans. on Automatic Control, vol. 26, no. 1, pp.47-65, 1981.
57. *Stability and Robustness of Multivariable Feedback Systems*, M. G. Safonov, Cambridge, MA, MIT Press, June 1980, ISBN-10: 0262693046.

58. “Shuttle Rendezvous and Proximity Operations,” Don Pearson (NASA/JSC), date unknown.

59. “Faster, Better, Cheaper: An Idea Without a Plan,” W. F. Tosney, Aerospace Corporation presentation, November 8, 2000, a February 2002 tutorial available at the INCOSE-Washington Metro Area Chapter OnLine Library, https://www.incose.org/.

60. “Skylab Lessons Learned As Applicable To A Large Space Station,” William C. Schneider, A dissertation submitted to the faculty of The School of Engineering and Architecture of the Catholic University of America For the Degree Doctor of Engineering, Washington, D.C., 1976.

61. NASA Document NASA TM X-64860, “MSFC Skylab Lessons Learned,” July 1974.

62. “Skylab Attitude Control System,” T. R. Coon and J. E. lrby, IBM Journal of Research and Development, 1976, Volume 20, Number 1, Page 58.

63. “Orbital Express Autonomous Rendezvous and Capture Sensor System (ARCSS) Flight Test Results,” Manny R. Leinz, Chih-Tsai Chen, Michael W. Beaven, Thomas P. Weismuller, David L. Caballero, William B. Gaumer, Peter W. Sabasteanski, Peter A. Scott, and Mark A. Lundgren, SPIE Defense and Security Symposium, 2008, Orlando, Florida, Proc. SPIE 6958, Sensors and Systems for Space Applications II, 69580A, May 1, 2008.

64. MIT’s Role in Project Apollo, MIT-IL R-700 Final Report, Volumes I-V, October 1971.

65. Landsat-6 Failure Investigation Final Report Summary, NOAA and Martin Marietta, January 16, 1995.

66. Report on Project Management in NASA, MCO Mishap Investigation Board, March 13, 2000.

67. “A Verification Procedure for MSC/NASTRAN Finite Element Models,” Alan Stockwell, NASA Contractor Report 4675, NASA Langley Research Center.

68. “NASA Space Vehicle Design Criteria (GNC), Effects of Structural Flexibility on Launch Vehicle Control Systems.” NASA SP-8036, February 1970.

69. “NASA Space Vehicle Design Criteria (Structures), Structural Interaction with Control Systems.” NASA SP-8036, February 1970.

70. “Control Structure Interation in Precision Pointing Servo Loops.” John Spanos, Journal of Guidance, Control, and Dynamics, Vol 12, No. 2, 989.

71. Lessons Learned from Seven Space Shuttle Missions, John Goodman, NASA CR-2007-213697, January 2007.

3.0 Appendices

Appendix A. Selected GN&C-Related Robotic Spacecraft Mishaps/Failures

Appendix B. GN&C-Related Lessons Learned (Extracted from the NASA LLIS)

Appendix C. GN&C-Related Best Practices from the NASA GSFC GOLD Rules Database

Appendix D. GN&C-Related Lessons Learned Extracted from the Aerospace Corporation Document, “100 Questions for Technical Review”

Appendix E. Gimbaled vs. Strapdown Inertial Systems

Appendix F. Apollo GN&C System Components

Appendix G. Use of Bond Numbers to Determine Liquid Slosh Regime

Appendix A. Selected GN&C-Related Robotic Spacecraft Mishaps/Failures

The following Robotic Spacecraft Mishaps/Failures are discussed in this Appendix:

A-1. Explorer-1 (1958)

A-2. Mariner-10 (1973)

A-3. Viking Orbiter (1975)

A-4. Mars Observer (1993)

A-5. Landsat-6 (1993)

A-6. Clementine (1994)

A-7. Lewis (1997)

A-8. GeoSat Follow-On (1998)

A-9. TOMS-EP (1998)

A-10. NEAR (1998)

A-11. WIRE (1999)

A-12. Mars Climate Orbiter (1999)

A-13. Mars Polar Lander (1999)

A-14. ACRIMSat (1999)

A-15. Terriers (1999)

A-16. X-43A (2001)

A-17. TIMED Satellite (2001)

A-18. CONTOUR (2002)

A-19. AQUA (2002)

A-20. GENESIS (2004)

A-21. DART (2005)

Note: Findings and recommendations from the mishap and failure reports are used to support the definition of several GN&C/ACS Engineering Best Practices.

A-1. Explorer-1 (1958)

Explorer-1 was the first U.S. artificial satellite. It was launched on January 31, 1958, on a modified Jupiter-C rocket by the Army Ballistic Missile Agency. Explorer-1 was injected into an orbit with a perigee of 224 miles and an apogee of 1,575 miles, having a period of 114.9 minutes. Its total weight was 30.7 pounds, of which 18.4 pounds were science instrumentation. The instrument section at the front of the satellite and the empty scaled-down Sergeant fourth-stage rocket casing orbited as a single unit, spinning around its long axis (minimum inertia axis) at 750 rpm. As such, it was classified a simple spin-stabilized satellite. Once on-orbit, Explorer-1 experienced attitude instability problems. Designed to be spin-stabilized about its minimum inertia axis, the vehicle was assumed to be inherently stable. This assumption was based upon the well-known dynamic property that rotation of a rigid body about the maximum or the minimum inertia axis is stable. The assumption that Explorer-1 was a rigid body was false. Energy dissipation in a set of flexible wire whip telemetry antennas had a destabilizing effect on the vehicle, and it eventually wound up in flat spin about its maximum moment of inertia axis.

A-2. Mariner-10 (1973)

As the Mariner 10 (MVM ’73) vehicle was nearing its encounter with Venus, an uncontrolled oscillation occurred due to spacecraft structural interaction with the ACS. The problem was first detected during a platform calibration sequence, which required a series of roll turns using roll gyroscope inertial control, and science scan platform motion. The result was a severe consumption of control gas that would have caused mission failure had it continued. The oscillation was due to a control instability exciting a structural mode of the spacecraft. The primary cause of the resonance was attributed to the flexibility of the solar panels.

An investigation concluded that spacecraft structural dynamical interactions with the ACS can be subtle and complex. The following recommendations were put forward as a result:

1. During the spacecraft design phase, consideration should be given to:
    a. Increasing the amount of analysis on and simulation of structural / control interactions.
    b. Placing additional or tighter controls on key parameters at interfaces between structures and attitude control.
    c. Establishing procedures for communicating key parameter data between subsystem engineers and analysts, initially and when changed.
2. In situations where there is significant uncertainty in simulations, models, or analysis results, the spacecraft subsystem software should be designed to accommodate changes late in the development, test, and post-launch periods. Techniques such as modular design and parameter tables vs. hard coding should be considered.
3. The capability to cope with this type of anomaly, by analysis and simulation, should be maintained throughout the mission.

Refer to NASA Public Lessons Learned Entry #0400 (Spacecraft Structure Dynamical Interaction with Attitude Control) for the detailed background on this particular anomaly.

A-3. Viking Orbiter (1975)

During pre-launch testing on the second Viking Orbiter (VO-2), a launch pad problem developed involving the FSW program and the Reaction Control System thrusters. The flight software, intended for use only after launch, contained within it a "safing sequence." The intent of the safing sequence was to automatically place the spacecraft in a safe state should some anomaly be detected. The safing sequence included commands to enable the Reaction Control System (RCS) and its thrusters.

In spite of procedural safeguards, a problem developed that inadvertently resulted in the issuance of the safing sequence while VO-2 was still on the launch pad. This, in turn, enabled the RCS thrusters. The ACS sensed the Earth's rotation, causing the RCS thrusters to fire in an attempt to compensate. Thruster firing continued until disabled by the test team, resulting in a significant loss of N2 attitude control gas. The launch was conducted without replacing the lost gas, rather than take the spacecraft down off the launch vehicle for replenishment. The safing sequence was also inadvertently issued several times during system test, but no adverse consequences resulted.

An investigation into this ground anomaly concluded that "when command sequences are stored on the spacecraft and intended to be exercised only in the event of abnormal spacecraft activity, the consequences should be considered of their being issued during the system test or the pre-launch phases." Had the ability of the safing sequence to enable the thrusters been constrained in some manner until after launch, for example, the VO '75 problem would not have occurred.

Refer to NASA Public Lessons Learned Entry # 0403 for the detailed background on this particular anomaly.

A-4. Mars Observer (1993)

The MO spacecraft was to be the first U.S. spacecraft to study Mars since the Viking missions of the mid-1970s. The MO fell silent on August 21, 1993, just 3 days prior to entering orbit around Mars, following the pressurization of the vehicle's propulsion subsystem. The MO utilized a bi-propellant propulsion method that employed monomethyl hydrazine (MMH) as the fuel and nitrogen tetroxide (NTO) as the oxidizer.

Because the telemetry transmitted from the Observer had been commanded off and subsequent efforts to locate or communicate with the spacecraft failed, the MO failure investigation board was unable to find conclusive evidence pointing to a particular event that caused the loss of the spacecraft.

However, after extensive analyses, the board reported that the most probable cause of the loss of communications with the spacecraft on August 21, 1993, was a rupture of the MMH fuel pressurization side of the spacecraft's propulsion system, resulting in a pressurized leak of helium gas and liquid MMH under the spacecraft's thermal blanket. The gas and liquid would most likely have leaked out from under the blanket in an asymmetrical manner, resulting in a net spin rate. This high spin rate would have caused the spacecraft to enter into "contingency mode," which interrupted the stored command sequence and thus did not turn the transmitter on.

Additionally, this high spin rate precluded proper orientation of the solar arrays, resulting in discharge of the batteries. However, the spin effect may be academic, because the released MMH would likely attack and damage critical electrical circuits within the spacecraft.

The board's study concluded that the propulsion system failure most probably was caused by the inadvertent mixing and the reaction of NTO and MMH within titanium pressurization tubing during the helium pressurization of the fuel tanks. This reaction caused the tubing to rupture, resulting in helium and MMH being released, thus forcing the spacecraft into a catastrophic spin and also damaging critical electrical circuits.

Based on tests performed at JPL, the board concludes that an energetically significant amount of NTO had gradually leaked through check valves and accumulated in the tubing during the spacecraft's 11-month flight to Mars.

In addition, the report listed other possible causes of the loss of the spacecraft as:

- Failure of the electrical power system, due to a regulated power bus short circuit.
- An over-pressurization of the NTO tank and subsequent rupture due to pressurization regulator failure.
- The accidental high-speed ejection of a NASA standard initiator device from a pyrotechnic valve into the MMH tank or other spacecraft system.

Among the other concerns noted by the investigation board were the following:

- A need to establish a policy to provide adequate telemetry data of all mission-critical events.
- Over-reliance on the heritage of spacecraft hardware, software and procedures for near-Earth missions, which were fundamentally different from the interplanetary MO mission.
- Deficiencies in systems engineering/flight rules.
- The lack of post-assembly procedures for verifying the cleanliness and proper functioning of the propellant pressurization system.
- A lack of understanding of the differences between the characteristics of ESA and NASA pyro-initiators.

The JPL board that also investigated the MO loss added another potential failure scenario:

- Loss of function that prevented both the spacecraft's main and backup computers from controlling its attitude.

A-5. Landsat-6 (1993)

The Landsat-6 (L6) spacecraft was launched on 5 October 1993 on a two-stage Titan-II booster from Vandenberg Air Force Base (VAFB) in California. L6 was the sixth spacecraft in the Landsat Program's series of Earth remote sensing satellites. The L6 spacecraft never achieved orbit following separation from the Titan-II and was a total mission loss.

The Landsat-6 spacecraft design employed a STAR-37XFP solid rocket Apogee Kick Motor (AKM) internal to the spacecraft to provide the last increment of orbital insertion velocity needed for L6 to attain its 705 km circular polar mission orbit. This was a similar orbit insertion strategy utilized many times before by the Landsat-6 spacecraft contractor on the Defense Meteorological Satellite Program (DMSP) and Television Infrared Observation Satellite (TIROS) military and civilian meteorological spacecraft. Effectively, with this insertion strategy, the Landsat-6 carried its own third-stage propulsion internally (the AKM) accommodated within the spacecraft along with the necessary ascent guidance software (AGS), which utilized inertial sensor outputs from the on-board IMU. After separating from the launch vehicle, the AGS would nominally serve to navigate and guide the L6 spacecraft into the nominal, or best available,

mission orbit. The AGS software also included the attitude control logic needed to command the pulsing of four 100-lbf thrust reaction engine assembly (REA) hydrazine thrusters. These REAs fired to produce sufficiently large control torques to counteract any de-stabilizing disturbance torques generated by the firing of the solid-fueled AKM.

The entire Ascent Phase was planned to take 40 minutes, at which time the AGS would hand over control of the spacecraft to the orbit mode software (OMS). Nominally, after AKM burn completion, the REAs would perform a small final orbital velocity trim maneuver (if deemed required by the AGS) and then be closed off for the mission duration. Shortly after that, the AGS would hand over to the OMS, the spacecraft's solar array would be deployed, and the rest of the nominal early-orbit mission operations sequence would be initiated.

Throughout the Ascent Phase of the mission, all real-time telemetered data from the Titan-II was nominal. There was no Landsat-6 spacecraft real-time telemetry available during ascent. The L6 was radio silent during ascent because its telemetry transmitter operated on the same frequency as the Titan-II telemetry transmitter. The real-time launch vehicle telemetry was deemed to be of the highest relative priority: so the Titan-II flew with its telemetry transmitter powered on while the L6 spacecraft had its telemetry transmitter powered off.

An 8-month investigation was jointly performed by both the government (NOAA) and the spacecraft contractor. The lack of any spacecraft telemetry from the Ascent Phase greatly hampered the failure investigation. Data from the Titan-II telemetry and radar data from a Moving Object Tracking Radar (MOTR) system at VAFB were extensively exploited to aid in the determination of the L6 failure root cause.

Titan-II telemetry data indicated that spacecraft separation from the booster occurred at the nominal time and place. All expectations were that contact with the spacecraft would be nominally established at the first ground station (Kiruna, Sweden) approximately 70 minutes after launch. This first contact with Landsat-6 was never established, and subsequent attempts to locate the spacecraft were futile. The inability to make contact with the Landsat-6 spacecraft, coupled with reports from other assets indicating reentry events downrange from the observed Titan-II booster stage reentry, led to the conclusion that the spacecraft had not achieved orbit following separation from the Titan-II.

The L6 failure investigation team concluded that the spacecraft experienced a rupture in its RCS hydrazine manifold. This ruptured hydrazine manifold rendered the spacecraft's REAs useless because the propellant could not reach the engines. The function of the four 100-lbf thrust REAs was to provide pitch and yaw attitude control torques to adequately stabilize the spacecraft during the firing of its solid-fueled AKM. The REAs were physically mounted at the four corners of the L6 aft equipment compartment. They were placed and aligned symmetrically about the spacecraft longitudinal mass centerline and symmetrically with respect to the nominal AKM thrust centerline. As was the case with the heritage DMSP and TIROS spacecraft, roll axis control toques would be provided by a set of low-thrust cold gas thrusters for complete three-axis control during the L6 AKM burn.

To satisfy requirements for launch safety, the hydrazine propellant was physically isolated from the REAs on the launch pad at liftoff and through most of the Ascent Phase by a set of two normally closed pyrotechnic valves, or pyrovalves. These pyrovalves were located between the tank holding the hydrazine monopropellant at a pressure of 420 psia and the REA engine

manifold. At the liftoff of L6, the upstream hydrazine tank side of the RCS was held at 420 psia and the downstream REA engine manifold side had only 16 psia inert helium gas. Nominally, during the Ascent Phase, the downstream side helium gas was to be vented by dry-cycling the REAs for 0.5 seconds just prior to the firing of the first pyrovalve. The two pyrovalves were nominally to be fired in sequence, one second apart, allowing the hydrazine to flow downstream from the tank to fill the REA engine manifold. Effectively, this meant the L6 spacecraft was launched with its REAs in a dry state.

This was a change from the heritage DMSP and TIROS launch configurations in which the REAs were not isolated from their hydrazine propellant tank and were in a wet state at liftoff. In this state, the entire REA engine manifold is filled with hydrazine and the only step needed to fire the REA to produce thrust is a valve "open" command. This wet REA pre-launch/liftoff RCS configuration apparently satisfied the launch safety requirements levied upon the DMSP and the TIROS heritage programs. Having the REAs in a wet state at liftoff did not satisfy the L6 launch safety requirements. This represented another change for L6 with respect to the DMSP and TIROS RCS heritage.

Lacking the control authority of the REAs to maintain stable attitude control, the spacecraft entered an un-controlled tumble during the AKM firing event. Consequently, the spacecraft did not accumulate a sufficient delta velocity from the AKM firing to attain an orbit about the Earth. The spacecraft re-entered the atmosphere south of the equator approximately 30 minutes after liftoff. The reentry of the spacecraft was validated by both a lack of a signal over the Kiruna ground station and the observations of other nation assets.

The L6 failure investigation revealed that although similar to the heritage DMSP and TIROS spacecraft designs, the L6 spacecraft required some mission-specific modifications to its RCS design. These modifications altered the heritage of the RCS subsystem.

The heritage RCS used on DMSP and TIROS needed to perform only two functions: 1) control spacecraft pitch and yaw attitude during the Ascent Phase, and 2) provide roll axis attitude control torques during the Ascent Phase and high-authority (relative to the reaction wheels used nominally) attitude control torques to remove any unexpected buildup of spacecraft momentum due to off-nominal disturbance torques experienced during on-orbit operations. The 100-lbf hydrazine-fueled REAs were part of the heritage design and were included to perform the Ascent Phase attitude control function. A set of eight 2-lbf cold gas nitrogen engine assembly thrusters were also part of the heritage RCS design and were included to perform the ascent roll control function and the on-orbit momentum management/disturbance torque control function.

However, unlike the heritage DMSP or TIROS missions, the L6 Earth remote sensing mission requirements dictated that the spacecraft have a propulsive capability to perform orbit altitude and orbit inclination maneuvers to precisely maintain the L6 ground track and equator crossing time per the top-level LANDSAT program mission requirements. The resultant L6 RCS flight hardware configuration therefore was modified to include a set of four 1-lbf hydrazine monopropellant orbit adjust engine (OAE) thrusters to provide the Delta-V required for maintaining the L6 orbit altitude and orbital inclination within the mission-level specified range.

Therefore the L6 RCS was an integrated system comprising both elements of the DMSP/TIROS heritage RCS and the new OAE hydrazine thrusters. This represented yet another change for L6 with respect to the DMSP and TIROS RCS heritage.

Failure Investigation Ground Testing

As part of the failure investigation, the spacecraft contractor performed multiple ground tests:

- RCS water hammer tests
- Pyrovalve pyroshock tests
- RCS system hydrazine adiabatic detonation/explosive decomposition tests
- Hydrazine explosive decomposition at PV actuation
- Hydrazine material compatibility tests

The body of test data generated provided the means to both postulate various scenarios for the Landsat-6 failure and, in turn, critically evaluate those scenarios. These tests played a very significant role in the failure investigation. The test data related to water hammer, adiabatic detonation and hydrazine explosive decomposition PV actuation were obtained in a high fidelity mock-up simulation of the flight RCS at the spacecraft contractor's facility. The system was extensively instrumented with high-frequency response pressure transducers capable of accurately measuring the short-duration, high-magnitude pressure spikes that an analytical transient flow model had predicted would occur.

A comprehensive program of RCS testing was conducted, using water first to measure the magnitude and location of the water hammer pressure spikes, then using hydrazine to see if the adiabatic compression (and therefore heating) by these pressure spikes of the helium gas in the lines was sufficient to cause the hydrazine to ignite and explode (adiabatic detonation). In most of the tests, rapid-acting electro-mechanical valves were used to simulate the pyrotechnic valves used in flight. This was done because of the quick turn-around time from test to test and because of the limited supply of pyrovalves.

However, the last series of ground tests, using hydrazine as the fluid, employed pyrovalves. These RCS mock-up tests were conducted following exactly the sequence employed during the L6 Ascent Phase. Specifically, the manifold from the tanks to the pyrovalves (PV-1 and PV-2) were filled with 420 psia water or hydrazine, while the manifold downstream of the valves to the REA thrusters were filled with l6 psia gaseous helium, simulating conditions from liftoff to beginning of the helium venting. Each test began with the 0.5 second venting of the downstream helium gas to vacuum through the simulated REAs and upon closing the REA valves, simultaneously firing PV-1, which released the 420 psia liquid into the now low pressure (1.7 psia) helium filled manifold (assuming PV-1 has functioned nominally). The liquid would get to the downstream side of PV-2 rapidly in these tests as all the other lines continued to fill, with short duration pressure spikes created at all the dead ends. PV-2 thus had hydrazine fuel on both sides of it before it was activated (i.e., fired) to open 1 second after the nominal firing of PV-1.

In one of these RCS mock-up ground tests (Test #11), a detonation event was produced.

L6 Failure Investigation Board (FIB) Conclusions & Recommendations

1. The L6 spacecraft experienced a ruptured hydrazine manifold. The ruptured manifold rendered the spacecraft's REA attitude control thrusters useless because fuel could not reach the engines. The failure first manifested as a large shock signature sensed by the booster instrumentation package, then as a low separation velocity between the Titan-II booster second stage and the L6 spacecraft, and finally as an inability to maintain attitude control during the AKM burn. As a consequence of tumbling during the AKM burn, the spacecraft

did not accumulate sufficient energy to attain orbit and instead reentered the atmosphere south of the equator, roughly 1808 seconds after liftoff. This conclusion is validated by the lack of Landsat signal acquisition at the Kiruna, Sweden, ground station and the observations of other national assets. The AKM burn itself was accepted as having occurred because of trajectory analysis linking the nominal trajectory with the reported/observed re-entry of L6.

2. The propulsion system conditions ground-tested during the failure investigation were shown to be capable of producing an explosive event of sufficient severity to rupture the pyrovalve manifold. An 8:1 relative difference between the shocks measured by booster accelerometers at PV-l actuation and PV-2 actuation have not been adequately explained by valve-to-valve variability or differences in the mounting of the pyrovalves to the spacecraft structure. The force of an explosion at PV-2 actuation could account for the difference.

3. A rupture of the 1/2-inch fuel lines at the PV-2 location was shown by analysis to be capable of reducing the fuel pressure at the REAs to virtually zero. Post-flight RCS mock-up ground testing (Test #11) was able to produce a detonation event. The pressure transducers at the REA locations in this ground test confirmed that there was no residual pressure in the manifold downstream of the rupture immediately after the RCS mock-up Test #11 detonation event. The loss of fuel pressure prior to commanding the REAs to perform the 5-second separation burn would account for the absence of substantial separation velocity as measured by booster accelerometers and ground tracking assets.

4. It is probable that the exact conditions of the fluid flowing around bends and past tees influences the amount of hydrazine frothing and the relative position of the compressed helium bubble with respect to PV-2. These non-repeatable processes could account for the lack of an explosion during one of the post-flight RCS mock-up ground tests (Test #13). It should also be noted that the fuel temperature for ground Test #11 (where a detonation event occurred) was 71 °F and the fuel temperature for ground Test #13 (no detonation) was 52 °F. It is possible that the difference in fuel temperatures contributed to the variability of the results obtained.

5. The investigators concluded that conditions existed that could have resulted in an explosive event at PV-2 actuation. It is not unreasonable to expect that such an explosive event occurred at PV-2 actuation during the Landsat-6 flight. The explosion would account for the high shock signature measured by the booster accelerometers and the lack of separation velocity. The resulting inability to provide control authority during AKM burn would explain the failure of the Landsat-6 spacecraft to achieve orbit.

6. The Joint L-6 FIB stated that it was beyond the scope of their task to investigate the mechanics of how the explosion occurred or which parameters are critical to preventing such explosions. It is reasonable to conclude that the Landsat-6 failure was due to an explosive event in the hydrazine system caused by conditions not previously reported to be capable of triggering adiabatic compression induced detonation of hydrazine.

The FIB made recommendations to be applied to future projects. Their stated intention was a maximum emphasis on the lessons learned from the loss of L6 and, with this intention, provided the following suggestions for improvements in testing and modeling a hydrazine fuel system and offer possible approaches for dissemination of lessons learned. Recommendations were made in three separate areas:

- Testing – Any newly designed hydrazine fuel feed system should be tested extensively. The test model should incorporate the actual flight sequences and flight equipment built to the flight drawings. This methodology may be the only way to mitigate the risk inherently incurred by the variability of the detonation controlling parameters. The test program should include more than one test using the planned flight sequence, flight, or flight-type components and the planned fuel at the expected environmental extremes. Particular attention should be given to the qualification and application of normally closed pyrovalves.
- Models and Research – During the system design phase, it is necessary to create models that closely resemble the flight system. The design team should perform sensitivity analysis to various parameters and predict test results. They must verify the flow regimes in each line and check for cavitation and water hammer pressures above 100 psi. The system must be designed so that gas-liquid phase interfaces are not trapped near any pyrovalves when they are actuated.

  A task force should be formed to address the best methodology for determining the parameters that designers must control to provide safe and failure-flee hydrazine feed systems. The task force should enlist membership from government, industry technical staff, and academia. Once the task force issues its recommendations for the research tasks, a funding profile should be established among the corporations and government agencies that will benefit from these results. All test results should be openly shared within the aerospace community.
- Launch – Although not related to the root cause of the Landsat-6 failure, implementation of the following recommendations would aid in the investigation of future launch or mission anomalies regardless of cause. Neither the booster vehicle nor satellite vehicle should be launched without telemetry active from liftoff to mission completion. Appropriate ground or aircraft telemetry receivers should be deployed to receive data for all critical events.

The details of the Landsat-6 failure investigation are contained in LS-6 Failure Investigation Final Report Summary from January 1995 [ref. 65].

A-6. Clementine (1994)

Clementine was a relatively low-cost mission with a primary objective of demonstrating emerging spacecraft technologies. The spacecraft design included several advanced technology innovations thought likely to have high payoff when applied to future small spacecraft missions. As a secondary objective, Clementine was designed to carry a limited suite of scientific instruments to survey the Moon and to fly past an asteroid.

The Clementine spacecraft was designed and developed using an acquisition and management philosophy similar to NASA's FBC approach being used at this time. Following a 22-month development phase, Clementine was launched in late January 1994 and operated by the Ballistic Missile Defense Organization within the DoD. Note that the Clementine spacecraft was the first U.S. space vehicle to depart the Earth's vicinity and fly to the Moon and beyond that was not managed or operated by NASA.

An unanticipated GN&C/fight software interaction caused the flight computer to "freeze," resulting in an uncontrollable spacecraft spin-up. This anomaly occurred after Clementine left

lunar orbit. A malfunction in one of the on-board computers caused a thruster to fire until it had used up all of its fuel, leaving the spacecraft spinning at about 80 rpm with no spin control.

A-7. Lewis (1997)

The Lewis spacecraft was procured by NASA via a 1994 contract with TRW Inc. as part of NASA's Small Satellite Technology Initiative (SSTI) Program. The SSTI Program was intended to validate a new approach to the acquisition and management of spacecraft systems by NASA. This effort was to use a new approach of FBC acquisition and management by NASA and the contractor. This provided for minimal government oversight in the implementation of the effort and shifted a larger responsibility to the contractor than was standard at that time. The concept was to implement the program using integrated product development teams that included members from industry, the science community, academia, and the government. The stated objectives were to reduce costs and development time of spacecraft for science mission applications. Specifically, the program was to demonstrate new small satellite design and qualification methods.

The Lewis spacecraft was launched on August 23, 1997. Contact with the spacecraft was subsequently lost on August 26, 1997. The spacecraft re-entered the atmosphere and was destroyed on September 28, 1997.

The FIB found that the loss of the Lewis spacecraft was the direct result of an implementation of a technically flawed ACS safe mode. This error was made fatal to the spacecraft by the reliance on the unproven safe mode by the on-orbit operations team and by the failure to adequately monitor spacecraft health and safety during the critical initial mission phase.

Specifically, the FIB concluded, the Lewis spacecraft had both a flawed ACS design and simulation.

Flawed ACS Design. The safe mode was required by TRW specification to maintain the spacecraft in a safe, power-positive orientation. This mode was to drive the solar panels to a predetermined clock position, to orient the spacecraft intermediate axis (the x-axis) toward the Sun and to maintain that orientation autonomously using thruster firings without ground station intervention for a minimum of 72 hours in mission (523 km altitude) orbit. This was implemented using a single two-axis gyroscope that was unable to sense rate about the x-axis. Therefore, when the spacecraft tried to maintain attitude control, a small imbalance, perhaps in thruster response, caused the spacecraft to spin up around the not-sensed x-axis. Because the spin was about an intermediate axis, the spin momentum started to transfer into the controlled principal axis (z-axis), causing the thrusters to fire excessively in an attempt to maintain control. The ACS processor was programmed to shut down the control system if excessive firings occurred. When both the A-side and the B-side thrusters had been shut down sequentially, the spin momentum that had been built-up in the intermediate (x) axis transferred into the principal (z) axis. This had the effect of rotating the spacecraft up to 90° in inertial space, causing the solar arrays to be pointed nearly edge-on to the Sun. The spacecraft then drained its battery at a significantly fast rate because of the power subsystem and thermal subsystem safe mode design.

Flawed ACS Simulation. The operations crew, relying on the ACS safe mode as validated by simulation, allowed the spacecraft to go untended for a 12-hour period. This reliance was ill-founded, because the simulation used to validate the ACS Safe Mode was flawed. The ACS

design heritage was initially based on the proven Total Ozone Mapping Spectrometer (TOMS) design. The expected system performance was analyzed using tools developed for the TOMS program. In fact, the Lewis control subsystem design was significantly more complex than TOMS because the Lewis spacecraft aligned its x-axis (intermediate/unstable), rather than its z-axis (principal/stable) of inertia toward the Sun in safe mode. When a Lewis design modified version of the TOMS simulation was run, neither a thruster imbalance nor an initial (albeit small) spin rate about the intermediate (roll) axis was modeled. The simulation was run for about twice the 72-hour requirement and demonstrated stability under the programmed conditions. An additional factor was that the simulation was done using mission mode parameters, not low-Earth transfer mode parameters representing the condition the spacecraft was actually in at the time of these operations. The mission mode represented a more stable attitude control condition.

Because of the programmatic experimental nature of the SSTI Program, the FIB was also tasked to review and assess the Lewis spacecraft acquisition and management processes to determine if they may have contributed to the failure. The FIB discovered numerous other factors that contributed to the environment that allowed the direct causes of the Lewis failure to occur. While the direct causes were the most visible reasons for the failure, the FIB concluded that the indirect causes were also significant. Many of these factors were attributed to a lack of a mutual understanding between the contractor and the government on fundamental programmatic and technical elements of the FBC acquisition/management approach. The following list of indirect contributors are to be taken in the context that the Lewis project was implemented under NASA's FBC model of system acquisition:

- Requirement changes without adequate resource adjustment.
- Cost and schedule pressures.
- Program Office move.
- Inadequate ground station availability for initial operations.
- Frequent key personnel changes.
- Inadequate engineering discipline.
- Inadequate management discipline.

The details of the Lewis failure investigation are contained in the Lewis FIB Report (1998).

A-8. GeoSat Follow-On (1998)

The GEOSAT Follow-On (GFO) program is the Navy's initiative to develop an operational series of radar altimeter satellites to maintain continuous ocean observation from the GEOSAT Exact Repeat Orbit. GFO is the follow-on to the highly successful GEOSAT-A. GFO is a 370 kg satellite that is three-axis stabilized with momentum wheels. It has a single solar array with one-axis articulation and hydrazine thrusters for orbit maintenance.

The spacecraft was launched on February 10, 1998, on a Taurus launch vehicle. The spacecraft tumbled instead of achieving the correct attitude. An analysis of early on-orbit spacecraft telemetry led the ground operation team to conclude that there was a polarity (sign) error in the ACS attitude control loop. This ACS polarity error was corrected via a simple and straight-forward uplinking of modified ACS control loop parameters in a FSWdata table. The satellite's attitude recovered within a few orbits and it was properly Sun-pointing within 0.02° with attitude rates of less than 0.006 °/s.

In addition to the ACS polarity problem described above the GFO also experienced some initial spacecraft hardware problems. There were problems with on-board flight computer resets, and the GPS receivers failed. With the failure of the GPS receivers, the primary means of both orbit determination and precision time tagging of the mission data were lost. A ground approach for time tagging the data was developed and implemented by June 1999. The computer reset problems were resolved in November 1999. On November 29, 2000, the Navy accepted the satellite as operational.

A-9. TOMS-EP (1998)

The Total Ozone Mapping Spectrometer-Earth Probe (TOMS-EP) is a NASA/GSFC science mission performing long-term daily mapping of the global distribution of Earth's atmospheric ozone layer.

TOMS-EP was launched into low-Earth orbit on a Pegasus XL booster on July 2, 1996. The spacecraft executed a series of Delta V burns to reach a 500 km circular Sun-synchronous mission orbit with an ascending node mean local time crossing of 11:18 AM. The data obtained from TOMS-EP were originally intended to complement science data taken from the ADEOS TOMS, which gave complete equatorial coverage due to its higher orbit. With the failure of ADEOS in June 1997, the orbit of TOMS-EP was boosted to 740 km and circularized to provide coverage that is almost daily.

On December 13, 1998. TOM-EP experienced a single event upset that caused the system to reconfigure and enter safe mode. This incident occurred 2.5 years after the launch of the spacecraft, which was designed for a two-year life. A combination of factors, including changes in component behavior due to age and extended use, unfortunate initial conditions, and the safe mode processing logic, prevented the spacecraft from entering its nominal long-term storage mode. The spacecraft remained in a high fuel consumption mode designed for temporary use. By the time the onboard fuel was exhausted, the spacecraft was Sun-pointing in a high-rate flat spin.

Although the uncontrolled spacecraft was initially in a power and thermal-safe orientation, it would not stay in this state indefinitely due to a slow precession of its momentum vector. A recovery team was assembled to determine if there was time to develop a method of de-spinning the vehicle and return it to normal science data collection. A three-stage plan was developed that used the onboard magnetic torque rods as actuators. The first stage was designed to reduce the high spin rate to within the linear range of the gyroscopes. The second stage transitioned the spacecraft from Sun-pointing to orbit-reference-pointing. The final stage returned the spacecraft to normal science operation. The entire recovery scenario was simulated with a wide range of initial conditions to establish the expected behavior. The recovery sequence was started on December 28, 1998, and completed by December 31. TOMS-EP was successfully returned to science operations by the beginning of 1999.

Additionally, CSS wiring and magnetic control loop phasing issues were found during early orbit checkout and corrected.

A-10. NEAR (1998)

The Near Earth Asteroid Rendezvous (NEAR) was designed to study the near Earth asteroid Eros from close orbit over a period of a year. NEAR was successfully launched February 17,

1996, to start its planned three-year cruise phase towards Eros. The spacecraft employed extensive autonomy because the round trip communication link (speed of light) time was up to 40 minutes long thereby precluding ground intervention during an emergency. As it approached Eros on December 20, 1998, the spacecraft began the first and largest of a series of rendezvous burns required for capture into orbit around the asteroid.

Almost immediately after the main engine ignited, the burn aborted, demoting the spacecraft into safe mode. Less than a minute later the spacecraft began an anomalous series of attitude motions, and communications were lost for the next 27 hours. Onboard autonomy eventually recovered and stabilized the spacecraft in its lowest safe mode (Sun-safe mode). However, in the process NEAR had performed 15 autonomous momentum dumps, fired its thrusters thousands of times, and consumed 29 kg of fuel (equivalent to about 96 meters/second in lost Delta-V capability). The reduced solar array output during periods of uncontrolled attitude ultimately led to a low-voltage shutdown in which the solid-state recorder was powered off and its stored spacecraft housekeeping telemetry data lost.

After reacquisition, NEAR was commanded to a contingency plan and took images of Eros as the spacecraft flew past the asteroid on December 23. A new burn was planned and executed on January 3, 1999, which would permit a second chance for rendezvous with Eros. The makeup burn placed NEAR on a trajectory to rendezvous with Eros on February 14, 2000, 13 months later than originally planned. The remaining fuel would be sufficient to carry out the original NEAR mission, but with little or no margin.

The cause of the abort itself was determined within 2 days of the event: the main engine's normal start-up transient exceeded a lateral acceleration safety threshold that was set too low. Compounding this error was a missing command in the onboard burn-abort contingency command script; this script error started the attitude anomaly. Fault protection software onboard NEAR correctly identified the problem and took the designed preprogrammed actions. While the fault protection actions did prevent complete battery discharge before the spacecraft recovered its proper Sun-facing orientation, they failed to prevent, and possibly exacerbated, the protracted recovery sequence.

The initial script error was not caught during software tests. Hardware-in-the-loop simulation could not test abort scenarios because the brassboards were difficult to use. Lacking a zero-gravity environment, a wrap-around simulation with a "truth model" is the only way to test a GN&C system. This requires meticulous attention to modeling of physical phenomena. The NEAR truth model was written by the flight team and mirrored all the incorrect physical models used to design the spacecraft GN&C algorithms. Although NEAR had a so-called independent V&V (IV&V) team for GN&C, the flight team gave them all the models. Consequently, there was no independence between the flight algorithms and the truth models used by either the design team or the V&V team.

Exactly how the anomalies propagated is unclear because a bus undervoltage wiped out data from the recorder, nor could the anomalous behaviors be reproduced on ground. During the emergency, the spacecraft fired its thrusters thousands of times. Fortunately, the fuel loss was tolerable because the thrusters were hardwired to fire for only fractions of a second. The mission was saved because the designers had added a watchdog timer to protect against fuel depletion during a software crash, a lesson learned from a previous deep space mission failure

(Clementine). NEAR went on to become the first spacecraft to orbit an asteroid, and the mission ended with a landing on Eros on February 12, 2001.

A-11. Wide-Field Infrared Explorer (1999)

WIRE, the fifth spacecraft developed under NASA's Small Explorers (SMEX) was launched into orbit on March 4, 1999, by a Pegasus XL booster. The WIRE ACS was a three-axis magnetic control system using a three-axis magnetometer for attitude sensing and a set of torque rods for control actuators.

The WIRE science instrument was designed to use a two-stage solid-hydrogen cryostat to keep its detector cooled to below 13 K throughout the primary mission phase. The cryostat was equipped to vent hydrogen "boiloff" gas from each of stages. The WIRE cryostat's secondary stage, given its predicted larger boiloff gas flow, was to be vented through a thrust nullifier device. This device is simply a matched pair of vents in a "tee" configuration designed to minimize the force and torque disturbances acting on the vehicle by releasing equal amounts of boiloff gas in opposite directions. However, the WIRE cryostat's primary stage simply used a simple open pipe as a boiloff vent.

Mission safety requirements dictated closing the cryogen boiloff vents during launch operations. Mission designers recognized, however, that the prompt opening of these vents was required shortly after launch to preclude over-pressure conditions within the cryostat dewar. This was necessary to vent the accumulated hydrogen that would have sublimated during the launch process. To accomplish this, real-time commands were transmitted early in WIRE's first ground contact to open the cryostat secondary stage vent. The primary stage vent was then opened a few minutes later via an on-board stored command. Non-reversible thermal actuators, under the control of the instrument pyro-controller unit, were used to open both vents.

Consistent with the way many space platforms operate in LEO, the WIRE did not have continuous real-time command and telemetry contact with its ground operations team. Contact with the WIRE spacecraft was to be made through a series of typically short (a few minutes each) passes overhead via a specific ground tracking station in a network of multiple globally distributed stations. The early-orbit operations concept dictated that the WIRE spacecraft, which was not equipped to use the Tracking and Data Relay Satellite System (TDRSS) for near-continuous contact, would nominally make real-time contact with ground stations for an average of 9 out of every 48 minutes. When certain ground stations were not available, this real-time contact time was reduced to 9 out of every 96 minutes. Stored spacecraft telemetry was to be downlinked at each ground contact, but this recorded data, which captures the vehicle's state of health between real-time contacts, would not be available to ground controllers until several hours into the mission.

The science instrument design also employed an ejectable shield over the telescope aperture to provide radiation and thermal protection. This shield's function was to minimize heat transfer into the instrument during early orbit operations, when the instrument would not otherwise be adequately isolated from the Earth albedo or sunlight. Nominally the shield was to have been ejected after successful three-axis attitude acquisition, also using non-reversible pyrotechnic actuators fired by the same instrument pyro-controller unit that commanded the vents open, on the third day of the mission.

Prior to the commanded opening of the secondary vent, the WIRE spacecraft dynamic behavior began to depart from nominal predictions. During the first ground contact, commands were transmitted per the mission plan to vent the cryostat hydrogen tank. Some spacecraft body axis angular rates were observed by the end of the 10-minute pass, but they were expected because of the tipoff dynamics from booster separation event and possibly the small amount of venting from the cryostat after the vent was opened. These angular tipoff angular rates were actively being nulled, and this was indicative of nominal ACS operation

However, at the next ground pass the spacecraft was observed to be tumbling at high rates. A review of stored telemetry showed the WIRE vehicle had experienced a continuous increase in spin rates between ground contacts. This increase in spin rates was neither predicted nor understood. At this point, the source of the disturbance toque producing the spin rate was unknown to ground controllers.

With the spacecraft in an uncontrolled tumble, the science instrument telescope, which at this point should have been pointed only to cold deep space, was most likely exposed to unexpected thermal inputs from Earth and Sun intrusions. Given this unanticipated situation where thermally hot objects were transiting through the unshielded telescope field of view, the heat load input rapidly sublimated the hydrogen cryogen. Analysis performed as part of the failure investigation indicated that the rapidly venting boiloff gas produced an average disturbance over five times the torque authority of the magnetic torque rod control actuators.

Ground controllers were able to verify proper input/output operation of the magnetic ACS, but it lacked sufficient control authority to dampen the spacecraft's tumble rates. Within 36 hours of launch, the instrument's four-month supply of cryogen was completely exhausted and the instrument detector was probably damaged by exposure to direct sunlight. At the end of the venting, the spacecraft was left spinning at about 53 rpm around the major moment of inertia axis (the body-X axis), with this axis pointing roughly inertial south. In this vehicle orientation, the solar array photovoltaic cells were illuminated by the Sun during half of each spin cycle and the spacecraft could be placed in a power positive configuration. This favorable situation permitted the ground operations team the opportunity to recover control of the vehicle after the cryogen was exhausted and the disturbance torque on the vehicle due to the boiloff gas venting ceased.

During the next five days, the spacecraft rates were damped using the digital form of the acquisition controller (the safehold mode) with only the Y and Z magnetic torquer bar rate damping terms enabled. Once the spacecraft spin rate had fallen to a low-enough value on March 11, the spacecraft was subsequently transitioned its normal on-orbit ACS mode on March 15. Throughout this process, the all spacecraft systems performed as expected. The WIRE spacecraft ultimately was put to use as an on-orbit engineering testbed.

The WIRE FIB concluded there was no failure of any one component that caused the WIRE mission failure, but rather a series of design and process mistakes. The FIB pointed to two basic mistakes: the root cause that started the series of events that led to WIRE's failure and a design flaw that allowed it to propagate. As usual in major failures, there were numerous contributing causes.

Root Cause: Instrument Pyro-Controller Electronics Unit

The root cause was determined to be a digital logic design error in the instrument pyro controller electronics unit. The box design was not well understood. This was especially true of the oscillator and field programmable gate array (FPGA) components start-up characteristics. When 28V power was applied to the pyro electronics box, a supposedly innocuous event, a 22A transient pulse was generated during the meta-stable state power-up region of the FPGAs and oscillator. The failure investigation revealed that as soon as the instrument pyro-controller box was powered up, it commanded all the actuators under its control to fire simultaneously for about 2 milliseconds, instead of according to the pre-programmed sequence. The effect was to arm and fire the vent actuators as well as the shield actuators, thus releasing the shield. This caused ejection of the instrument shield and the opening of at least one cryogen vent in the process. The primary vent may not have been opened at the time, since its thermal actuator takes longer to fire than the pyrotechnic actuators used to eject the shield. The shield was not intended for release until much later, when the spacecraft was stable and pointing at the correct target in cold deep space. The separation of the shield at this stage of the mission was independently confirmed by NORAD when it observed, starting between the first and second ground passes, multiple objects in the vicinity of the WIRE spacecraft.

Propagating Cause: Vent Design and Location

The cryogenic system had a correctly designed boiloff vent using a tee. This should have ensured that no torques were imparted to the spacecraft when the cryogen was vented, no matter what the vent rate was. However, the vent was improperly oriented such that on one side the cryogen boiloff gas flow impacted some spacecraft structure. The tee exit had been placed as close as possible to the exit point on the cryostat to minimize the pressure, and therefore the temperature, inside the cryostat secondary tank. This had the effect of providing a large unbalanced torque on the spacecraft during the high vent rates, causing the rapid tumble. A low vent rate, which was expected, would not have caused this problem. The vent design and location were not reviewed because they were done after the cryostat was built and delivered. The potential design problem was observed, but based on the expected low vent rates, the project saw no need to change the design just a few months before launch.

The project had made the connection early in the WIRE design cycle between the loss of cryogen and the reduction of mission life. It was known that if the spacecraft pointed at the Earth without the instrument shield it would lose a day of mission life for every hour the spacecraft tumbled. Therefore, a major driver in the ACS design was to keep WIRE out of that condition. Additionally, there was a specification on the ACS to control the spacecraft for nominal cryogen venting disturbance. However, the connection between the two was never made. That is to say, the loss of a day's worth of cryogen per hour meant a vent rate that would be 24 times the nominal vent rate. Even knowledge of the high vent rate might not have changed the design of the ACS. A magnetic torquing system is generally not robust compared to a high thrust cold gas system. It might not have been practical to change the design. However, had this connection been made, more attention might have been paid to the vent design and impingement issue. The ACS was probably designed to handle any imbalances between well-balanced tee vents. The worst-case venting scenario was not considered.

For failure investigation details, refer to the WIRE MIB Report (1999).

A-12. Mars Climate Orbiter (1999)

The MCO mission objective was to orbit Mars as the first interplanetary weather satellite and provide a communications relay for the MPL, which was due to reach Mars in December 1999. The MCO spacecraft was launched on December 11, 1998, atop a Delta II launch vehicle from Cape Canaveral Air Force Station, Florida. Nine and a half months after launch, in September 1999, the spacecraft was to fire its main engine to achieve an elliptical orbit around Mars. It then was to skim through Mars' upper atmosphere, performing an aerobraking maneuver for several weeks to transition into a low circular orbit. Friction against the spacecraft's single 5.5-meter solar array was to have lowered the spacecraft altitude as it dipped into the atmosphere, reducing its orbital period from more than 14 hours to 2 hours.

On September 23, 1999, the MCO was lost when it entered the Martian atmosphere on a lower than expected trajectory. The actual loss of the spacecraft occurred following the spacecraft's entry into Mars occultation during its Mars Orbit Insertion (MOI) maneuver.

The MCO MIB determined that the root cause for the loss of the MCO spacecraft was the failure to use metric units in the coding of a ground software file, SM_FORCES (small forces), used in trajectory models. Specifically, thruster performance data in English units instead of metric units were used in the software application code. A file called Angular Momentum Desaturation (AMD) contained the output data from the SM_FORCES software. The data were required to be in metric units per existing software interface documentation, and the trajectory modelers assumed the data met the requirements.

During the nine-month journey from Earth to Mars, propulsion maneuvers were periodically performed to remove the accumulated angular momentum buildup in the on-board reaction wheels. These AMD events occurred 10-14 times more often than expected by the operations navigation team. This was because the MCO solar array was asymmetrical relative to the spacecraft body as compared to Mars Global Surveyor (MGS), which had symmetrical solar arrays. This asymmetric effect significantly increased the solar pressure-induced momentum buildup on the spacecraft. The increased AMD events, coupled with the fact that the angular momentum (impulse) data were in English rather than metric units, introduced small errors in the trajectory estimate over the course of the nine-month journey.

At the time of Mars insertion, the spacecraft trajectory was approximately 170 kilometers lower than planned. As a result, MCO was either destroyed in the atmosphere or re-entered heliocentric space after leaving Mars' atmosphere.

The root cause of the MCO failure was determined by the MIB to be failure to use metric units in the coding of a ground software file, "Small Forces," used in trajectory models. The loss of spacecraft was due to an engineering units conversion error. The ground software did not convert the thruster impulse-bit parameter from English "lbf-second" units to specified SI units of "N-second," a factor of 4.45. The MIB recognized that mistakes occur on spacecraft projects. However, sufficient processes are usually in place to catch these mistakes before they become critical to mission success. Unfortunately, the root cause was not caught by the processes in place for the MCO project.

The MIB also cited the following contributing causes:

1. Undetected mismodeling of spacecraft velocity changes.

2. Navigation Team unfamiliar with spacecraft.
3. Trajectory correction maneuver No. 5 not performed.
4. System engineering process did not adequately address transition from development to operations.
5. Inadequate communications between project elements.
6. Inadequate Operations Navigation Team staffing.
7. Inadequate training.
8. V&V process did not adequately address ground software.

The MIB made some specific GN&C-related observations, demonstrating that a robust systems engineering team and processes were not in place:

1. Navigation requirements set at too high a management level, insufficient flowdown of requirements, and inadequate validation of these requirements.
2. Several significant system and subsystem design and development issues, uncovered after the MCO launch (e.g., the star camera glint issue and the inability of the navigation team to receive telemetry from the ground system for almost six months).
3. Inadequate IV&V of MCO ground software (i.e., end-to-end testing to validate the small forces ground software performance and its applicability to the software interface specification did not appear to be accomplished). There was a failure to complete—or completion with insufficient rigor—of the interface control process, as well as verification of specific ground system interfaces.
4. Absence of a process, such as a fault tree analysis, for determining what could go wrong during the mission.
5. Inadequate identification of mission-critical elements throughout the mission (e.g., the mission criticality of specific elements of the ground software that impacted navigation trajectory was not identified).
6. Inadequate criteria for mission contingency planning (e.g., without the development of a fault tree, there was no basis for adequate contingency planning).
7. Insufficient autonomy and contingency planning to execute TCM no. 5 and other mission-critical operations scenarios.
8. A navigation strategy that was totally reliant on Earth-based, Deep Space Network tracking of the MCO as a single vehicle traveling in interplanetary space. Mission plans for the MPL included alternative methods of processing this data, including using near simultaneous tracking of a Mars-orbiting spacecraft. These alternatives were neither implemented nor operational at the time of the MCO encounter with Mars. The MIB found that reliance on single-vehicle, Deep Space Network tracking to support planetary orbit insertion involved considerable systems risk, due to the possible accumulation of unobserved perturbations to the long interplanetary trajectory.

For additional technical details on the root cause and factors contributing to the MCO failure refer to the MCO Phase I Report, released November 10, 1999.

Subsequent to issuing its final report identifying the root cause and factors contributing to the MCO failure, the MCO MIB was given the additional task of deriving lessons learned from that failure and from other failed missions—as well as some successful ones—and creating a formula for future space mission success.

The MCO mission was conducted under NASA's FBC philosophy, which was developed with the objective of enhancing innovation, productivity, and cost-effectiveness of space missions. As part of this second task, the board found that while the FBC approach allowed NASA to do more with less, the success of the FBC model was tempered by the fact that some projects and programs put too much emphasis on cost and schedule reduction (e.g., the "Faster" and "Cheaper" elements of the paradigm). At the same time, these projects and programs failed to instill sufficient rigor in risk management throughout the mission life cycle. The board concluded these actions increased risk to an unacceptable level on these projects.

The details of the board's findings, observations, and recommendations relative to improving space mission success within the context of the FBC paradigm are documented in its second report, "Report on Project Management in NASA" [ref. 66]. This report puts forward a new vision, "Mission Success First," which entails a new NASA culture and new methods of managing projects to ensure mission success.

A-13. Mars Polar Lander (1999)

The mission objective of the MPL was to soft land near the South Pole and study meteorology and soil properties, analyze water and carbon dioxide in the atmosphere and soil, and photograph the surroundings. It was to be the first Mars landing outside the tropics of the Martian northern hemisphere. Communications with the spacecraft ceased, as planned, at the start of atmospheric entry and nothing more was ever heard from the lander. The FIB concluded that the most likely failure mode was that the lander's GN&C system, which controlled the firing of the RCS engines used to decelerate the vehicle to a soft landing, would interpret the vibrations as the lander's legs were deployed as an indication of surface contact and consequently shut down RCS engines too early, causing the vehicle to crash to the surface. It was believed that a software error occurred in how data and signal from the touchdown sensor were used. An end-to-end test of the landing system was deleted from the MPL test sequence due to schedule pressures. MPL was therefore a complete mission loss.

A-14. ACRIMSat (1999)

The Active Cavity Radiometer Irradiance Monitor satellite (ACRIMSat) was launched on December 21, 1999. The 253-lb (115-kg) spacecraft was launched on a Taurus launch vehicle rocket from VAFB. The ACRIMSat mission science objective was to study the amount of sunlight falling on Earth's atmosphere, oceans, and land to help scientists improve predictions of long-term climate change.

ACRIMSat was a spin-stabilized spacecraft. Specifically, it was a major axis spinner designed to point its spin axis towards the Sun. The spacecraft was launched in the accelerometer-based damping mode to damp nutation. Almost immediately, the pointing error started increasing rapidly as the spacecraft spin axis moved away from the Sun. The spacecraft averaged roughly a 70-degree pointing error, and battery charge was rapidly decreasing. The spacecraft was commanded into the backup CSS-based Sun damping mode. The Sun-sensor-driven damping left

the spin axis hanging off at a point approximately 15 degrees from the Sun. The spacecraft was power-positive, but unable to perform its intended science mission.

Troubleshooting revealed a polarity error in the accelerometer loop had caused the initial 70-degree divergence. The 15-degree offset under Sun-sensor-driven damping was caused by a software error in transcribing an "X" subscript in the control algorithm as a "Z" subscript in the flight code. After correcting these two mistakes, Sun pointing was automatically switched to the Fine Sun Sensor, which was expected to reduce the pointing error to less than 0.25 degrees. However, the residual pointing error stabilized at about 1.5 degrees. Troubleshooting of this third anomaly revealed a units error in the Sun sensor geometrical dimensions and several typographic errors in the stray light correction algorithm. After corrective FSW code patches were uplinked to the spacecraft, the ACRIMSat Sun pointing attitude control mode finally met its performance requirements.

A-15. Terriers (1999)

The Tomographic Experiment using Radiative Recombinative Ionospheric Extreme ultraviolet and Radio Sources (TERRIERS) satellite was successfully launched at 1:09 a.m. EDT, May 18, 1999, from VAFB aboard an Orbital Science Corp. Pegasus rocket. TERRIERS was a Student Explorer Demonstration Initiative (STEDI) mission managed for NASA by the Universities Space Research Association of Columbia, Maryland. TERRIERS was one of three NASA-sponsored missions developed under STEDI.

Following launch ground controllers observed the spacecraft losing power and determined that it was unable to orient itself properly to allow its solar panels to fully face the Sun. Telemetry data indicated that the spacecraft was in the correct orbit and spinning appropriately about the right axis.

A recovery team of spacecraft engineers and other experts was formed to develop a plan to return the satellite to operation. Initially, the ground recovery team was hopeful that the satellite's solar panel would slowly charge the spacecraft and that in time the satellite would have enough power to turn itself on. The recovery team continued for some time to attempt radio contact with the spacecraft, to no avail.

The subsequent failure investigation determined the cause of the TERRIERS failure to be an ACS polarity error that had the effect of off-pointing the spacecraft's solar array by 180°. Complete mission failure was therefore due to inadequate end-to-end ACS polarity testing in the flight conjuration.

A-16. X-43A (2001)

The X-43A was the first flight attempt conducted as part of NASA's Hyper-X Program, which was initiated in 1996 to advance hypersonic air-breathing propulsion and related technologies from laboratory experiments to the flight environment. This program was designed to be a high-risk, high-payoff program. The X-43A was to be the first flight vehicle in the flight series. The X-43A was a combination of the Hyper-X Research Vehicle (HXRV), HXRV adapter, and Hyper-X Launch Vehicle (HXLV), referred to as the X-43A stack.

The first X-43A flight attempt was conducted on June 2, 2001. The HXLV was a rocket-propelled launch vehicle modified from a Pegasus launch vehicle stage one (Orion 50S)

configuration. The HXLV was to accelerate the HXRV to the required Mach number and operational altitude to obtain scramjet technology data. The trajectory selected to achieve the mission was at a lower altitude and subsequently a higher dynamic pressure than a typical Pegasus trajectory. This trajectory was selected due to X-43A stack weight limits on the B-52 carrier aircraft.

The HXLV solid rocket motor ignition occurred 5.19 seconds after being dropped from the B-52, and the mission proceeded as planned through the start of the pitch-up maneuver at 8 seconds. During the pitch-up maneuver, the X-43A stack began to experience a control anomaly at approximately 11.5 seconds, characterized by a diverging roll oscillation at a 2.5 Hz frequency. The roll oscillation continued to diverge until approximately 13 seconds when the HXLV rudder electromechanical actuator stalled and ceased to respond to autopilot commands. The rudder actuator stall resulted in loss of yaw control that caused the X-43A stack sideslip to diverge rapidly to more than 8 degrees. At 13.5 seconds, structural overload of the starboard elevon occurred. The severe loss of control caused the X-43A stack to deviate significantly from its planned trajectory, and the vehicle was terminated by range control 48.57 seconds after release.

The X-43A MIB attributed the mission failure to the HXLV and concluded that the root cause was that the vehicle control system design was deficient for the trajectory flown due to inaccurate analytical models (e.g., Pegasus heritage and HXLV), which overestimated the system margins. The key phenomenon that triggered the failure was the divergent roll oscillatory motion at a 2.5 Hz frequency. The divergence was primarily caused by excessive control system gain. A second phenomenon that was a consequence of the divergent roll oscillation was a stall of the rudder actuator that accelerated the loss of control. Neither phenomenon was predicted by preflight analyses.

The analytical modeling deficiencies resulted from a combination of factors. It should be noted that the X-43A MIB considered a very comprehensive definition of the term “models,” to include system architecture, boundary conditions, and data.

The X-43A failure occurred because the control system could not maintain the vehicle stability during transonic flight. The vehicle instability was observed as a divergent roll oscillation. An effect of the divergent roll oscillation was the stall of the rudder actuator. The stall accelerated loss of control, which resulted in loss of the X-43A stack. The rudder actuator stalled due to increased deflections that caused higher aerodynamic loading than preflight predictions. The deficient control system and under-prediction of rudder actuator loads occurred due to modeling inaccuracies.

To determine the cause of the X-43A mishap, in-depth evaluations of the Pegasus and HXLV system and subsystem models and tools, as well as extensive system-level and subsystem-level analyses, were performed by the MIB. To support the analyses, extensive mechanical testing (fin actuation system) and wind tunnel testing (6 percent model) were required. The major contributors to the mishap were modeling inaccuracies in the fin actuation system and aerodynamics and insufficient variations of modeling parameters (i.e., parametric uncertainty analysis). Pegasus heritage and HXLV-specific models were found to be inaccurate.

Fin actuation system inaccuracies resulted from:

- Discrepancies in modeling the electronic and mechanical fin actuator system components
- Under prediction of the fin actuation system compliance used in the models.

Aerodynamic modeling inaccuracies resulted from:

- Error in incorporation of wind tunnel data into the math model
- Misinterpretation of wind tunnel results due to insufficient data
- Unmodeled outer mold line changes associated with the Thermal Protection System.

Insufficient variations of modeling parameters were found in:

- Aerodynamics
- Fin Actuation System
- Control System

Less significant contributors were errors detected in modeling mass properties. Potential contributing factors were found in the areas of dynamic aerodynamics and aeroservoelasticity. Linear stability predictions were recalculated using the corrected nominal models. Stability gain margins were computed for all axes. Aileron gain margin (roll axis) was examined in particular and showed a sizeable reduction from the 8 dB preflight prediction. Model corrections led to a revised prediction of less than 2 dB at nominal conditions. This was well below the requirement of a 6 dB gain margin. Although this reduction was significant and close to instability boundaries, the revised prediction was still stable. This meant that nominal model corrections alone were insufficient to predict the vehicle loss of control and that parameter uncertainty had to be included. Accounting for parameter uncertainties in the analyses replicated the mishap. This was confirmed by nonlinear time history predictions using the 6-DoF flight dynamics simulation of the X-43A stack.

The X-43A MIB concluded that no single contributing factor or potential contributing factor caused this failure. The flight failure was only reproduced when all of the modeling inaccuracies with uncertainty variations were incorporated in the system level linear analysis model and nonlinear simulation model.

The details of the X-43A failure investigation are contained in the X-43A MIB Report (2003).

A-17. TIMED Satellite (2001)

The Thermosphere, Ionosphere, Mesosphere, Energetics and Dynamics (TIMED) spacecraft was launched on December 7, 2001 into LEO. TIMED is a 600 kg spacecraft that employs a three-axis zero-momentum ACS. The spacecraft has large solar arrays. All the subsystems on TIMED worked well, with the exception of a number of initial on-orbit ACS subsystem problems. These were quickly overcome, and the mission is now in the operational phase performing its science mission.

Momentum Unloading Control Logic Sign Error Problem

The first ACS problem encountered was a polarity error in the control loop used to perform the unloading (i.e., “dumping”) of accumulated angular momentum in the reaction wheels. This loop used magnetic torque rods, a magnetometer, and an inertial reference unit (IRU) to control and maintain momentum levels within the capability of the reaction wheels to accommodate. Shortly after separation from the launch vehicle, the ground operation team observed a steady increase in spacecraft system momentum. The situation was rapidly assessed, and a sign error was discovered in the magnetic torque rod control logic. However, no straightforward approach was available to correct the problem, such as changing a sign in momentum unlading control logic

path the ACS flight software. In addition, there were no simple means of disabling the torque rod actuators that were effectively working to increase system momentum. The ground operators determined, given the ACS architecture hardware/software interfaces, that the only way to disable commands to the torque rods was to power off the magnetometer. A temporary corrective measure for the control logic sign error was quickly formulated. It consisted of inverting the signs on the magnetometer biases and scale factors that were stored on-board as updateable ACS FSW parameters. The system momentum was observed to decrease once the sign inversion was implemented. The spacecraft rates did not exceed 2.5 degrees/second during this anomalous event, and the vehicle was maintained throughout in a power-positive state. The fact that the ground operations team had continuous, or near-continuous, early-orbit real-time command and telemetry contact with the TIMED spacecraft, via the TDRSS, allowed them to first observe and then react in a timely manner to this potentiality dangerous ACS sign error anomaly.

Sun Sensor Orientation Problem

When coming out of eclipse and seeing the Sun for the first time, the TIMED spacecraft was commanded to reorient to point toward the Sun. Depending upon the initial attitude, this maneuver could take up to 20 minutes. At the end of the eclipse, the spacecraft began to reorient itself as expected. However, after 20 minutes it showed no signs of settling out; commanded wheel torques showed an unexpected gyration occurring.

After an examination of telemetry containing raw Sun sensor measurements and solar wing currents, the ground operations team determined that the spacecraft had settled into a quasi-stable attitude with the x-axis generally pointed at the Sun. It appeared that the spacecraft was attempting to point this axis at the Sun rather than the desired Sun-pointing axis. What was fortunate for TIMED was that one of its large solar arrays was illuminated by the Sun and electrical power was being produced. Battery charging was being performed, and the spacecraft remained in a power-positive (an thermal-safe, as well) state for multiple orbits. The spacecraft had placed itself into a state not unlike a safe hold mode transition and maintained it.

With the spacecraft in this pseudo-safe hold mode, the ground operation team diagnosed the nature of the ACS problem using all means at their disposal: ACS flight hardware drawings, ACS FSWcode/data, and photographs of the spacecraft taken during the I&T phase. Attention was focused upon on each of the four Sun sensors, and an assessment was made of how the sensors were mounted and tested as well as how they were interfaced to the ACS FSW code. This scrutiny revealed the source of the ACS pointing problem. Based upon what was seen in a I&T photo of the Sun sensors, it appeared that the sensors were not mounted as designed.

Two Sun sensors on the hot side, which was to be pointed at the Sun during safe hold mode, were mounted 90 degrees from what was expected. However, the “cold” side sensors were correctly oriented.

The solution to the problem of having the hot side Sun sensors erroneously rotated from their expected orientation involved a change to the ACS FSW code. New parameters representing the orientation/alignment of the Sun sensors were designed and uplinked to the TIMED satellite flight computer. Sufficient on-orbit verification testing of this new FSW code was subsequently performed as part of the spacecraft’s early-orbit checkout phase.

The investigation into determining the root cause of this Sun sensor orientation problem revealed that although specific ACS phasing (i.e., polarity) tests had been performed during the spacecraft I&T phase, they had not been performed with the satellite in its actual flight configuration. The Test as You Fly engineering best practice had not been adhered to in this case. The root cause had to do with physical configuration of the spacecraft in the I&T facility when the ACS team performed pre-launch polarity testing. The two hot side Sun sensors were mounted to a panel on the y-axis side of the spacecraft. However, this particular panel was also the main panel through which the internal access to the spacecraft was attained during I&T operations. Consequently, the panel was removed and not in its flight configuration during most of the I&T activity. The two Sun sensors were temporarily hung off to the side. Unbeknownst to the ACS team, the orientation in which they were hung did not agree with the orientation they would have in flight. The investigation also revealed a breakdown in technical communications between the ACS and I&T teams. On one hand the ACS team did not inquire about the Sun sensor orientations, and conversely the I&T team did not communicate information about the two sensors that were temporarily off to the side. Moreover, there apparently was no documentation specifically denoting the desired orientation. Thus the ACS Sun sensor polarity tests were unintentionally and erroneously performed with the spacecraft in a non-flight configuration.

CSI problem

The TIMED satellite had two modes of operation: Sun-pointing and nadir-pointing. The former is used in spacecraft safe hold, while the latter is the science attitude, as is the one normally used on-orbit for data taking.

During the early on-orbit performance evaluation of the TIMED nadir pointing attitude control mode (“normal mode”), a CSI issue was observed. An unexpected 0.1 Hz oscillation in the 1 Hz real-time rate and wheel torque data occurred. However, the high data rate telemetry, which is sampled at 10 Hz, temporarily stored on-board, then downlinked to the ground, indicated the actual frequency of the structural oscillation was 2.1 Hz. It appeared that aliasing, due to 1 Hz sampling of the real-time telemetry, had created the fictitious 0.1 Hz. A scrutiny of the spacecraft’s modal frequencies from the structural finite element modeling confirmed that one of the solar array bending modes was being excited.

A subsequent investigation indicated that early in the TIMED ACS controller design phase, the structural flexible modes were given a cursory review to assess the potential for any CSI problems that might detrimentally impact ACS stability. The lowest structural mode frequency was 0.25 Hz while the controller bandwidth was 0.01 Hz, and with a decade or more separation between them, no further analysis was performed. A formal frequency domain analysis was not undertaken, and a suitable fidelity flexible-mode model was deemed unnecessary for the existing time domain simulation. These were serious omissions.

Filtering of the gyroscope data to protect against CSI problems had been recommended during design reviews. Such bending mode filtering was in fact implemented in the safe hold mode controller but not in the normal mode nadir-pointing control loop. The latter decision was based on the desire to avoid filtering the gyroscope information before inputting it into the Kalman filter used to perform spacecraft attitude estimation. It was an oversight not to filter the gyroscope data prior to use in the normal mode nadir-pointing ACS controller.

Post-launch investigations into this unanticipated CSI problem revealed a significant modal gain from the 2.1 Hz mode, which actually changes in frequency from 2.0 to 2.6 Hz over the 90 degree range of solar array motion each orbit. This finding was obtained via evaluation and a refinement of the spacecraft's structural finite element model using actual flight data. A frequency domain analysis demonstrated the unstable nature of this flexible mode for the given controller gain set and incorporation of the structural model in the time-domain simulation yielded results that correlated well with on-orbit telemetry data. The conclusion was that a complete and rigorous analysis of the flexible modes during the controller design would have exposed the problem discovered on-orbit, and it could have been eliminated pre-launch. The solution was to design and implement a low-pass Butterworth digital filter in the ACS FSW. After detailed frequency domain analyses, with time domain simulation concurrence, the proper filter coefficients and controller gains were selected to successfully alleviate the structural oscillation problem.

Spacecraft Residual Magnetic Dipole

Also during the early-orbit checkout phase, it was observed that momentum buildup was occurring at an unpredicted and relatively rapid rate. Based on momentum control parameters and the expected momentum buildup, the expectation was for momentum dumping to take place about once per day. In actuality, momentum dumping was occurring about 10 times per day. An analysis revealed an apparent spacecraft residual magnetic dipole of significant size and also that external torques were consistently tracking the magnetic field over an orbit period. The later piece of evidence strongly linked the issue to a magnetic cause. The residual dipole was estimated to be 10 A-m^2 and was determined to be primarily in the +y axis spacecraft direction. This phenomenon did not impact overall ACS operation. The observation can be made, however, that a pre-launch test to actually measure the spacecraft residual magnetic dipole would most likely have exposed this issue and allowed it to be given the attention it deserved before flight.

Root Cause and Other Contributing Factors

On February 11, 2002, a MIB was convened to investigate the anomalies. The MIB reported to the GSFC PMC on May 17, 2002, and August 28, 2002. TIMED met the minimum mission success criteria on April 22, 2002.

It has since been acknowledged that there was a breakdown in the APL G&C test processes that led to these anomalies. The possession of good processes for I&T alone does not guarantee success. They must be implemented correctly.

The MIB convened to investigate the GN&C post-launch anomalies concluded that these were consequences of inadequate procedures. The conclusion was that the root and/or contributory cause in all four anomalies were related to the lack of management processes. The observation was made that APL relied on the knowledge and integrity of key staff in lieu of a more process-oriented approach. Members of the GSFC technical staff observed that the processes used at the spacecraft I&T level were inconsistent with those used at GSFC. However, the contract did allow APL to use their own methods and procedures whenever possible if they met statement of work requirements. APL does have processes, but acknowledged these were not appropriately followed in the GN&C area.

A-18. CONTOUR (2002)

The Comet Nucleus Tour (CONTOUR) spacecraft was launched on July 3, 2002, and intended to encounter at least two comets. Following launch, the spacecraft remained in an eccentric Earth orbit until August 15, 2002, when an integral STAR 30BP Solid Rocket Motor (SRM) was fired to leave orbit and begin the transit to the comet Encke.

The mission design did not provide for telemetry coverage during the SRM burn, and no provision was made to observe the burn optically. CONTOUR was programmed to re-establish telemetry contact with the ground following the burn. However, no signal was received and attempts to contact CONTOUR were unsuccessful. Ground observations identified what appeared to be three separate objects on slightly divergent trajectories near but behind CONTOUR's expected position. Further attempts to contact CONTOUR were unsuccessful, and NASA concluded that the spacecraft had been lost.

Because of the lack of telemetry and observational data during the SRM burn, the MIB concentrated on a review of available design, manufacture, testing, and operations documentation. Although it could not unequivocally determine the proximate cause of the failure, the board identified a number of possible root and proximate causes.

The probable proximate cause was identified as overheating of the spacecraft by the SRM motor exhaust plume impingement. Alternate proximate causes included catastrophic SRM failure and loss of spacecraft dynamic control.

Root causes were identified as 1) CONTOUR Project reliance on analysis by similarity, 2) an inadequate systems engineering process, and 3) an inadequate review function. Significant observations included 1) lack of telemetry during a mission-critical event; 2) significant reliance on subcontractors without adequate oversight, insight, and review; 3) inadequate communication between the CONTOUR Project and SRM vendor; and 4) the SRM vendor's use of analytic models that were not specific to the CONTOUR spacecraft.

The details of the CONTOUR failure investigation are contained in the CONTOUR MIB Report (2003).

A-19. AQUA (2002)

The Aqua spacecraft was launched May 4, 2002, on a Delta II 7920-10L expendable launch vehicle from the Western Test Range at VAFB with a planned mission lifetime of six years. Stellar positions as measured by the spacecraft star trackers and ephemeris data uplinked from the ground are used in the onboard computer (OBC) attitude determination. All Aqua instrument teams use the downlinked OBC attitude quaternion for science data processing, so the onboard attitude solution accuracy is extremely important.

Soon after the Moderate Resolution Imaging Spectroradiometer (MODIS) instrument calibration was completed, the MODIS team identified a large yaw attitude oscillation (greater than 100 arcseconds) correlated with orbital period by comparing the MODIS observational data with known geolocation references. Several possibilities were explored, including ground data processing errors, thermally induced science instrument or attitude sensor alignment shifts, or other science instrument anomalies. After several weeks of analysis by a combined investigation

team, the MODIS yaw anomaly was finally traced to an inconsistency between the OBC star catalog and the OBC ephemeris.

The OBC ephemeris is uplinked daily and the onboard star catalog is stored in Mean of J2000 (M-J2000) coordinates. But the star positions were incorrectly changed to Mean of Date (MoD) coordinates by applying a precession correction in the OBC FSW prior to their use in the onboard attitude determination process. The precession correction is used to compensate for the periodic motion (~25,000 years) of the Earth's rotation axis relative to the ecliptic plane, but was unnecessary since the two original coordinate systems were compatible.

The difference between M-J2000 coordinates and MoD coordinates (i.e., precessed star positions) varies approximately 50 arcseconds/year and had grown to approximate ±150 arcseconds for the current time difference between the two coordinate systems (~3 years between 2000 and 2003). The coordinate system inconsistency caused the yaw oscillations because the OBC target attitude quaternion was derived from the OBC ephemeris (M-J2000), but the attitude was computed from MoD star positions. The coordinate system discrepancy resulted in an ecliptic latitude dependency and manifested primarily as yaw motion, although roll and pitch were also affected. The solution was to generate a software patch eliminating the star position precession correction in the onboard FSW.

The inconsistency between the onboard coordinate frames was not found during pre-flight software testing because the V&V simulation was not developed independently of the GN&C design simulation. After launch, the attitude determination in ground-based solutions did not detect the yaw attitude excursions because the ground used ephemeris-independent quaternions. However, once the coordinate system mismatch was found and the software patch uploaded, the yaw pointing error soon settled down to within the required +/- 25 arcseconds 3 sigma.

A-20. Genesis (2004)

Genesis was the fifth in NASA's series of Discovery missions, and the first U.S. mission since Apollo to return extraterrestrial material to Earth for study. The purpose of the Genesis mission was to collect samples of solar wind and return them to Earth. JPL was the managing Center; the California Institute of Technology was designated the principal investigator and project team leader. Los Alamos National Laboratory provided the science instruments, and Lockheed Martin Corporation (acting through Lockheed Martin Space Systems) was the industrial partner and provided the spacecraft and sample return capsule. JPL and Lockheed Martin Astronautics conducted mission operations.

Launched on August 8, 2001, Genesis was to provide fundamental data to help scientists understand the formation of our solar system. Analysis of solar materials collected and returned to Earth would give precise data on the chemical and isotopic composition of the solar wind.

On September 8, 2004, the Genesis sample return capsule drogue parachute did not deploy during entry, descent, and landing operations over the Utah Test and Training Range. The drogue parachute was intended to slow the capsule and provide stability during transonic flight. After the point of expected drogue deployment, the sample return capsule began to tumble and impacted the Test Range at 9:58:52 MDT, at which point vehicle safing and recovery operations began.

On September 10, 2004, the Associate Administrator for the Science Mission Directorate established a Type A MIB as defined by NASA Procedural Requirements 8621.1A, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping, to determine the cause and potential lessons from the incident. The board was chartered to determine the proximate cause of the failure, identify root causes, and develop recommendations to strengthen processes within NASA's Science Mission Directorate to avoid similar incidents in the future.

Additionally, the MIB was to determine the adequacy of contingency response planning and the appropriateness of the actual contingency response, to include the safing and securing of the spacecraft and the science payload and the protection of response personnel.

The board determined the proximate cause of the mishap to be that the G-switch sensors were in an inverted orientation, per an erroneous design, and were unable to sense sample return capsule deceleration during atmospheric entry and initiate parachute deployments.

The board found that deficiencies in the following four pre-launch processes resulted in the mishap:

- The design process inverted the G-switch sensor design.
- The design review process did not detect the design error.
- The verification process did not detect the design error.
- The Red Team review process did not uncover the failure in the verification process.

The board identified several root causes and major contributing factors that resulted in the design inversion of the G-switch sensors and the failures to detect it. The root causes and contributing factors fall into six categories, some of which contributed to more than one of the above process errors.

Inadequate Project and Systems Engineering Management

A lack of involvement by JPL Project Management and Systems Engineering in Lockheed Martin Space Systems spacecraft activities led to insufficient critical oversight that might have identified the key process errors that occurred at Lockheed Martin Space Systems during the design, review, and test of the spacecraft. This process was consistent with the Faster, Better, Cheaper philosophy of the time and approved by the Discovery Program.

Inadequate Systems Engineering Processes

Multiple weaknesses within the Genesis Systems Engineering organization resulted in requirements and verification process issues that led to the failure. The MIB recommended adding a thorough review of all systems engineering progress, plans, and processes as part of existing major milestone reviews. This recommendation was written to enforce discipline and critical assessment in the systems engineering organizations of future projects. Recommendations regarding systems engineering also addressed the issues raised by the inadequate project and systems engineering management root causes by compelling a commitment by project management to support an adequate systems engineering function.

Inadequate Review Process

All levels of review, including the Genesis Red Team review, failed to detect the design or verification errors. It was the MIB's position that technical reviews have become too superficial and perfunctory to serve Science Mission Directorate needs. The technical review

recommendations in this mishap report were targeted at significantly strengthening the directorate's review process.

Unfounded Confidence in Heritage Designs

Genesis Management and Systems Engineering and the Genesis Red Team made a number of errors because of their belief that the G-switch sensor circuitry was a heritage design. Further, the prevalent view that heritage designs required less scrutiny and were inherently more reliable than new designs led to the mishap. The MIB addressed the systemic problem of inappropriate faith in heritage designs by recommending review and verification of heritage designs to the same level expected of new hardware/software.

Failure to Test as You Fly

Several issues led to the lack of proper testing of the G-switch sensors, including a failure to treat the G-switches as sensors, which ultimately led to the mishap. The MIB's recommendations to strengthen the review process within the Science Mission Directorate partially addressed this issue, as well as a recommendation to require a test as you fly plan and a phasing test plan for all directorate projects.

FBC Philosophy

As demonstrated by several failures, NASA's use of the FBC philosophy encouraged increased risk-taking by projects to reduce costs. Although NASA Headquarters had solicited and selected Genesis under the FBC paradigm, the way JPL chose to implement the Genesis Mission substantially reduced insight into the project's technical progress. This precluded JPL from ensuring that the project was executed within the range of previously successful mission implementation practices, thereby adding additional risk. The Discovery Program Office accepted these arrangements implicitly by way of the selection and subsequent management review processes.

The potential pitfalls of this approach became clear when the MCO and MPL missions failed. Although much has been done within the Science Mission Directorate to correct FBC issues, the board recommended that when establishing appropriate levels of budgetary and schedule reserve, the Science Mission Directorate give greater consideration to overall maturity, launch constraints (e.g., short window planetary vs. others), and complexity.

MIB members based several recommendations on their experience with on-going Science Mission Directorate Systems Engineering and technical review issues. The board also considered previous failure investigations. Most of the recommendations center on improving the technical review process of new designs, heritage designs, and Systems Engineering. Instead of creating more reviews, the Board recommended more effective reviews that identify requirements, design, verification, and process issues early to avoid costly overruns or tragic failures.

It appeared highly likely to the MIB that due to the dedicated efforts of the Genesis Recovery and Curation Teams and the nature of the sample collection materials, most of the Genesis science goals will be met. However, the board believed this fortunate outcome should not reduce the importance of the lessons learned for future missions.

The details of the GENESIS failure investigation are contained in GENESIS MIB Report (2006).

A-21. DART (2005) – Publicly Releasable Findings

On April 15, 2005, the Demonstration of Autonomous Rendezvous Technology (DART) spacecraft was successfully deployed from a Pegasus XL rocket launched from the Western Test Range at VAFB. DART was designed to rendezvous with and perform a variety of maneuvers in close proximity to the Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM) satellite, without assistance (i.e., autonomously) from ground personnel.

DART performed as planned during the first eight hours through its launch, early orbit, and rendezvous phases, accomplishing all mission objectives up to that time, even though ground operations personnel noticed navigation system anomalies. During proximity operations, however, the spacecraft began using much more propellant than expected. Approximately 11 hours into what was supposed to be a 24-hour mission, DART detected that its propellant supply was depleted, and it began a series of maneuvers for departure and retirement. Although it was not known at the time, DART had actually collided with MUBLCOM 3 minutes and 49 seconds before initiating retirement.

Because DART failed to achieve its main mission objectives, NASA declared a "Type A" mishap and convened a MIB chaired by Scott Croomes of NASA's Marshall Space Flight Center (MSFC). A "Type A" mishap designates a NASA mission failure that exceeds a government loss of $1 million. This requires the most detailed level of investigation. In DART's case, none of the 14 requirements related to the proximity operations phase—the critical technology objectives of the mission—were met. However, the other portions of the DART mission, including the launch, early orbit, rendezvous, departure, and retirement phases, were completely successful. Out of a total 27 defined mission objectives, DART fully or partially met 11.

After the collision, both spacecraft remained in orbit. Because of this, no physical spacecraft remains were available for examination. However, other evidence was available for use by the MIB. The board investigated the mishap and determined its underlying causes based on hardware testing, telemetry data analysis, and numerous simulations. From its investigation, the MIB developed two timelines: one for DART's premature retirement and another for DART's collision with MUBLCOM.

After addressing causes related to both timelines, the MIB developed and documented in a formal report recommendations aimed at avoiding such occurrences in the future. Additional recommendations were added to the report through endorsement letters generated by the Exploration Systems Mission Directorate (ESMD) and the Office of Safety and Mission Assurance (OSMA).

NASA has completed its assessment of the DART MIB report, which included a DoD classification review. The report was found to be NASA-sensitive but unclassified, because it contained information restricted by ITAR and EAR. As a result, the DART mishap investigation report was deemed not releasable to the public. The following provides an overview of publicly releasable findings and recommendations regarding the mishap.

Dart Project Background

Proposed by Orbital Sciences Corporation (OSC) in response to a 2001 NASA Research Announcement from the Second Generation Reusable Launch Vehicle (2GRLV) Program, DART was selected by NASA as a high-risk technology demonstration project. The DART

contract was awarded in May 2001 to OSC within a broad NASA Research Announcement (NRA 8-30). The proposed cost of the DART mission was $47 million.

Later, in November 2002, the 2GRLV Program was redefined and became two new programs, the Orbital Space Plane Program and the Next Generation Launch Technology Program. DART, along with other flight demonstration projects, was transferred to the OSP Program. In the process, increased emphasis was placed on DART, because automated rendezvous technology was considered critical in supporting the potential future needs of the ISS Program.

In January 2004, after President George W. Bush announced the Vision for Space Exploration to explore the moon, Mars, and beyond, the OSP Program was canceled. Because of its relevance to the in-space assembly of certain exploration architecture concepts, however, the DART Project was continued. Because of the project's maturity at that time (its original target launch date was 2004), DART became NASA's first flight demonstration of new exploration capability. The DART mission was eventually launched on April 15, 2005, and cost $110 million.

The Dart And MUBLCOM Spacecraft

The DART spacecraft combined two systems. The forward segment contained DART-specific systems including a propulsion tank, reaction control system thrusters, batteries, communications equipment, and the AVGS. The AVGS, the mission's primary sensor, would collect navigation data while DART was close to MUBLCOM. The DART's aft portion was the fourth stage of a Pegasus launch vehicle, which included an avionics assembly and the Hydrazine Auxiliary Propulsion System (HAPS).

The AVGS would gather data from laser signals reflected off targets mounted on MUBLCOM and use these signals to calculate relative bearing and range data (i.e., the direction and distance from DART to MUBLCOM). When the DART-mounted AVGS was within 200-500 m of MUBLCOM, it was expected to provide only bearing measurements. When the AVGS was within 200 m of its target, it was expected to provide not only bearing, but also range and relative attitude (orientation of a spacecraft relative to an external reference) data.

Other navigational sensors that were to work in concert with the AVGS included two Global Positioning System (GPS) receivers on DART and a GPS receiver on MUBLCOM. DART would use data from these GPS receivers to determine position and velocity relative to MUBLCOM. Based on an intricate combination of data from all navigational sensors, on-board software would guide DART while it was in proximity to MUBLCOM. DART was not designed to receive commands from the ground, an approach considered philosophically consistent with the objective that DART be a demonstration of autonomous technology.

The MUBLCOM satellite was DART's rendezvous target. OSC launched MUBLCOM in 1999 for DARPA. Following completion of its original and primary mission, MUBLCOM remained in orbit in good operational condition.

The DART Mission Plan

The intent of DART was to demonstrate that a pre-programmed and unaided spacecraft could independently rendezvous with a non-maneuvering and cooperating satellite. A series of 27 objectives for a successful mission were developed and divided among four defined mission phases: 1) the launch and early orbit phase, 2) the rendezvous phase, 3) the proximity operations phase, and 4) the departure and retirement phase.

Launch and Early Orbit Phase

During the launch phase, the DART spacecraft, coupled with its Pegasus launch vehicle, would be flown to an altitude of 40,000 feet over the Pacific Ocean aboard a carrier aircraft. Following release, the three-stage Pegasus rocket would ignite, carrying DART into an initial parking orbit below MUBLCOM. From there, it would begin a series of navigation system checks, verifying position estimates for itself and its target, MUBLCOM.

Rendezvous Phase

During the mission's rendezvous phase, after completing systems checks, DART would fire its HAPS thrusters to move into a second phasing orbit or rendezvous. The HAPS burn would be timed to position DART below and behind MUBLCOM in preparation for the next phase. Among other things, NASA intended to demonstrate that a comparison of position and velocity data from GPS receivers in two spacecraft would be accurate enough to guide the "chaser" spacecraft (DART) to a position within the effective range of a proximity operations navigational sensor such as the AVGS.

Proximity Operations Phase

During the proximity operations phase, a series of scheduled maneuvers would move DART into MUBLCOM's orbit, first at a position about 3 km behind, and then about 1 km behind the target. When it was 1 km behind MUBLCOM, DART was programmed to evaluate AVGS performance through a series of precise close-range maneuvers. These maneuvers included various pre-planned holds (i.e., station-keeping periods at designated points in space), a collision-avoidance maneuver at a pre-determined position, and a maneuver to determine at what distance from MUBLCOM the AVGS tracking data could no longer be acquired.

Departure and Retirement Phase

After completing its proximity operations maneuvers, DART would perform a departure burn to move it away from MUBLCOM, expel its remaining fuel, and place itself into a short-lifetime retirement orbit in compliance with NASA safety standards.

Description of the Mishap

During the actual DART mission, all went as expected throughout the launch and early orbit phases. The vehicle successfully completed its rendezvous phase as well, placing itself into a second staging orbit about 40 km behind and 7.5 km below MUBLCOM, even though ground operators began to notice an irregularity with the navigation system.

When DART began its transfer out of the second staging orbit to begin proximity operations, ground operators observed that the spacecraft was using significantly more fuel than expected. It became clear that the mission would likely end prematurely because of exhausted fuel reserves. Because DART had no means to receive or execute uplinked commands, the ground crew could take no action to correct the situation.

During the series of maneuvers designed to evaluate AVGS performance, DART began to transition its navigational data source from the GPS to AVGS as planned. Initially, the AVGS supplied only information about MUBLCOM's azimuth (i.e., angular distance measured horizontally from the sensor boresight to MUBLCOM) and elevation relative to DART. However, as DART approached MUBLCOM, it overshot an important waypoint, or position in

space, that would have triggered the final transition to full AVGS capability. Because it missed this critical waypoint and the pre-programmed transition to full AVGS capability did not happen, the AVGS never supplied DART's navigation system with accurate measurements of the range to MUBLCOM. Consequently, DART was able to steer towards MUBLCOM, but not to accurately determine its distance to MUBLCOM. Although DART's collision avoidance system eventually activated 1 minute and 23 seconds before the collision, the inaccurate perception of its distance and speed in relation to MUBLCOM prevented DART from taking effective action to avoid a collision.

Less than 11 hours into the mission, DART collided with MUBLCOM. MUBLCOM did not appear to experience significant damage, and the impact actually pushed it into a higher orbit. Shortly after the collision, DART determined that it was nearly out of maneuvering fuel and initiated its pre-programmed departure and retirement maneuver. DART's departure and retirement phase proceeded per the original plan, and MUBLCOM regained its operational status after an automatic system reset that resulted from the collision.

Identifying Mishap Causes and Recommending Solutions

NASA's major goal in performing mishap investigations is to improve safety by identifying the proximate and root causes of a mishap and by providing recommendations to prevent future occurrences of similar events. If any one of the proximate causes were removed from the chain of events leading to the mishap, then the mishap would not have occurred. By analyzing *why* each of the proximate causes occurred, an MIB can identify root causes that may be common to other systems. The following summarizes the mishap causes identified by the DART MIB.

Causes of DART's Premature Retirement

The proximate cause of DART's premature retirement was that DART used up its maneuvering fuel (pressurized nitrogen gas) before it could complete its objectives. The MIB found that a repeated pattern of excessive thruster firings in response to incorrect navigational data onboard DART caused the higher than expected fuel usage. Ultimately, DART spent too much fuel as it continuously carried out corrective maneuvers while steering itself towards MUBLCOM, thus causing a premature end to the mission.

Normally, a spacecraft's software-based navigational system operates by constantly estimating its position and speed and comparing these estimates with measurements from its navigational sensors. If the estimate and the measured position agree, then the software can issue the correct commands to the maneuvering thrusters to guide the spacecraft along its desired flight path.

In DART's case, the MIB determined that the first cause for its premature retirement occurred when the estimated and measured positions differed to such a degree that the software executed a computational reset. By design, this reset caused DART to discard its estimated position and speed and restart those estimates using measurements from the primary GPS receiver.

Careful examination of the software code revealed that upon reset, the velocity measurement from the primary GPS receiver was introduced back into the software's calculations of the spacecraft's estimated position and speed. If the measured velocity had been sufficiently accurate, the calculations would have converged and resulted in correct navigational solutions. However, DART's primary GPS receiver consistently produced a measured velocity that was offset or "biased" about 0.6 meters per second from what it should have been. This had the

unfortunate effect of causing the calculations, which were being performed autonomously, to once again diverge until the difference became unacceptable to the pre-programmed computer logic. Once the limit as to how much the calculations could differ was reached, the software executed another reset. As a result, this cycle of diverging calculations followed by a software reset occurred about once every three minutes throughout the mission. These continual resets caused the incorrect navigational data that prompted excessive thruster firings and the higher than expected fuel usage.

The reason an incorrect velocity measurement from the primary GPS receiver was introduced into the software's calculations during a reset was because the software fix for this known "bug" had never been implemented by the DART team. In addition, the software model that simulated the receiver during preflight testing assumed that the receiver measured velocity perfectly. However, even with the incorrect velocity data being introduced into the calculations at each reset, the MIB determined that the navigational software's design was also inadequate. The design requirements stated that the measured velocity data only had to be accurate to within 2 meters per second (positive or negative). In reality, the design was incapable of accommodating a measured velocity with that much error, and the actual, erroneous data from the primary GPS receiver was off by less than 1 meter per second.

Yet even that deficiency was not enough to cause the continual calculation divergences and resets. An additional feature in the computational logic known as "gain" controlled how much the calculations were based on the estimated position and speed versus the measured position and speed. The gain determined how much "weighting" the two types of data (i.e., estimates versus measurements) received in the final calculations of differences.

The MIB concluded that the gain was set at an inappropriate level such that the calculations could never converge once the initial reset happened. The pre-programmed gain setting, which was changed late in the spacecraft's development, caused the logic to "trust" the estimated data more than it reasonably should have. This change did not undergo proper testing and simulations to verify the effects of the weighting. During analysis of pre-flight test data following the mishap, the MIB demonstrated that with the original (higher) gain setting, the string of repeated diverging calculations and software resets would have been broken.

In summary, the persistent, inaccurate navigational information that caused DART's premature retirement resulted from a combination of 1) an initial, unacceptable, calculated difference between DART's estimated and measured position that triggered a software reset; 2) the introduction of an uncorrected erroneous velocity measurement into the calculation scheme; 3) a navigational software design that was overly sensitive to erroneous data; and 4) the use of incorrect gain control in the calculation scheme.

Contributing to the premature retirement mishap was the nature of the design approach used for DART's guidance system. To make corrections to its flight path, DART's guidance system used continual, course-correcting thruster firings rather than a limited number of specific, mid-course correction maneuvers. DART's guidance system was not as capable as the second guidance approach, which could have handled divergent navigation estimates more effectively. While DART's guidance approach contributed to the mishap, it did not directly cause it to occur.

Additionally, the MIB found that the on-board computer logic that determined the remaining amount of maneuvering fuel during the mission significantly over-estimated the usage rate. This

factor caused DART to declare that the fuel was at its lower limit when in fact about 30% of the fuel was still in the tank. The MIB's analysis showed that this much fuel, had it been available for use, would have allowed the mission to continue for some minutes, but not long enough to complete the mission objectives, given the navigational problems (even if the collision had not occurred).

Causes of DART's Collision with MUBLCOM

The collision with MUBLCOM was caused by the inaccurate navigation system performance as described above coupled with increasingly accurate azimuth and elevation information from the AVGS. This had the effect of lining up MUBLCOM in the crosshairs of DART's guidance system at a time when the system lacked the ability to accurately control the distance between the two spacecraft. This condition existed because DART's pre-programmed logic for switching to AVGS distance measuring capability required the spacecraft to fly into an undersized, imaginary sphere (waypoint) along the flight path 200 m behind MUBLCOM. The MIB's analysis of the telemetry data from the flight shows that DART missed this 6.3 m radius spherical envelope by less than 2 m. The reasons for this inadequately-designed logic include the unanticipated potential for navigational errors and a lack of adequate design review.

When DART missed the critical waypoint for switching to full AVGS capability, it continued moving toward MUBLCOM. DART's design included a means of collision avoidance, but its capability proved ineffective. The software logic for collision avoidance was dependent on the same navigational data source as the guidance system. The impact of this dependency was that DART's calculated position and speed did not match its actual position and speed. In fact, at the time of collision, DART was flying toward MUBLCOM at 1.5 m/s while its navigational system thought it was 130 m away and retreating at 0.3 m/s. The collision avoidance design approach never anticipated the possibility that the navigational data would be this inaccurate.

Summary of Root Causes and Recommendations

DART was a one-time project. Because of this, the MIB did not propose specific design changes for the DART spacecraft. The formal mishap report contains detailed recommendations for the root causes that should prevent similar mishaps in the future.

The following summarizes root causes and recommendations formally addressed by the MIB:

- **High-Risk, Low-Budget Nature of the Procurement**

  DART was selected by NASA as a high-risk, low-budget technology demonstration under an NRA. The government procured only the data, and set broad requirements. Most of the detailed design decisions about how to meet those requirements were left to the discretion of the contractor.

  In DART's case, OSC carried over many of DART's design features from the Pegasus launch vehicle approach. For example, the software architecture, which consisted primarily of a pre-programmed, timed sequence of fixed commands, worked adequately for a launch vehicle, but as was eventually found by the MIB, was not able to respond adaptively while performing autonomous in-space operations with unanticipated inputs.

  The MIB recommended that the NRA acquisition approach be used for procuring only the initial conceptual design for technically complex, high-priority flight missions. Further, it

was recommended that the subsequent mission spacecraft design, development, and operations contracts use government-controlled, detailed specifications, and provide for a greater degree of control over key design decisions.

NASA Headquarters, in its review of the MIB report, disagreed with this MIB finding. The ESMD endorsement letter noted that "the NRA is a viable procurement instrument for future flight experiments if there is appropriate peer review of the concept(s) and appropriate management rigor."

- **Training and Experience**

  In the case of DART, a lack of training and experience led the design team to reject expert advice because of the perceived risks of implementing the recommendations. In turn, this led to inadequate navigation system design and testing. The DART MIB recommended that NASA centers with technical responsibility for rendezvous operations obtain an independent capability assessment. Center management should develop recruitment, retention, and training goals to fill any skill gaps. Finally, in NASA's source selection process, the training and experience of contractor teams should be evaluated.

  Despite its problems, the MIB noted the value of conducting a mission like DART. The "hands on" experience gained from actual flight system design and operation is crucial to overcoming knowledge deficiencies in autonomous spacecraft rendezvous techniques.

- **Lessons Learned Analysis**

  Even though the DART team lacked training and experience, many of DART's inadequacies could have been addressed through review and proper application of mission experience and data (i.e., lessons learned) documented from previous NASA projects.

  The MIB recommended revising NASA's engineering peer review procedures to require an independent check of how the project team has analyzed and acted upon "lessons learned" from previous missions.

- **GN&C Software Development Process**

  The MIB determined that one of the root causes of the mishap was an inadequate GN&C software development process. Changes to the flight code and simulation models were often incorporated without adequate documentation. In one case in particular, a change to the navigation system's reset logic was made that introduced the use of GPS velocity (as measured from the primary GPS receiver) as the new, estimated DART velocity whenever a reset occurred. This then became the only instance in which this particular parameter was to be accepted directly into the navigation system's logic.

  Most of the DART team was unaware that the GPS velocity output was to be used in this way by the navigation system's software. Because this was thought to be an unused parameter, personnel responsible for testing the receiver's performance and using the mathematical component models never realized the need to correct the problem with the biased velocity measurement or include the bias in the receiver's simulation model. Because of this, the velocity output of the receiver hardware and that of the simulated receiver did not match. As a result, the pre-flight simulations failed to reveal the adverse effect of the inaccurate velocity measurement from the primary GPS receiver during the mission.

In another case, an omitted units conversion caused an error in a simulation math model. This error was discovered after most HITL system testing had been completed. The late discovery was due to the inadequate GN&C software development process.

In response to its findings, the MIB recommended revising NASA policy to clarify that simulations and math models used to validate FSW must be verified and validated to the same rigorous level as the FSW itself. In addition, NASA software design standards should be revised to prevent unused parameters resident in the code from adversely affecting the FSW performance.

- **Systems Engineering**

  For the DART mishap, the MIB determined that an inadequate system-level integration process failed to reveal a number of design issues contributing to the mishap. In some cases, there was insufficient system-level understanding of the potential effects of complete or partial loss of functionality of relevant subsystems. Performance requirements for critical capabilities, such as collision avoidance, were not detailed enough to preclude numerous possible design interpretations, not all of which would lead to a system that worked correctly.

  The MIB recommended that NASA continue development of a NASA procedural requirements document for systems engineers, as well as require certification of systems engineers. Project and program managers should also be required to have extensive experience and training in systems engineering.

  OSMA's MIB endorsement letter states, "The MIB report clearly indicated that inadequate systems engineering (including a lack of implementation of software requirements, configuration control, validation of math models and testing) was a significant causal factor in the mishap. The report demonstrates that this was a failure to implement existing (NASA) engineering requirements, standards and practices." Consequently, it further recommended that the Office of the Chief Engineer consider performing independent audits or reviews of NASA program and project compliance with NASA systems engineering requirements, currently under development, as a supplement.

- **Schedule Pressure**

  Schedule pressure was identified as the cause for the inadequate testing of a late change to the navigation logic's gain setting. Correction of the units conversion error in the simulation math model described earlier led to a lowering of the gains setting to improve the expected proximity operations performance based on mission simulations. However, because the gain change happened so close to the planned launch, it was never adequately tested. The MIB determined that the pressure to maintain a scheduled launch was the root cause for the decision to forego testing of the change using the flight hardware and software. Adequate testing after the change would have revealed the problem with the lowered gain setting.

  As a result of this finding, the MIB recommended establishing a set of checks and balances to ensure that technical discipline is maintained throughout the entire development process, up to and including the launch and operations phase. Flight projects should develop and be able to report upon measures of flight readiness. Program or project plans for high-priority flight missions should require management checks to ensure that safeguards are in place against launching an improperly or incompletely-verified vehicle configuration.

- **ITAR Restrictions**

  In the case of DART, the MIB concluded that insufficient technical communication between the project and an international vendor due to perceived restrictions in export control regulations did not allow for adequate insight.

  To better facilitate critical data exchange in key mission areas, the MIB recommended revising NASA policy to require program and project managers to confer with Export Control officials to evaluate the adequacy of data exchange arrangements. Likewise, detailed Export Control training should be required for project personnel involved in interactions with foreign entities.

- **Technical Surveillance/Insight**

  The MIB determined that in several instances, the NASA DART insight team failed to identify issues that led to the mishap because of an inadequate assessment of project technical risk and insufficiently defined areas of responsibility. For example, examination of raw test data and performance of independent tests of some flight components by the government insight team were defined by NASA project management to be out-of-scope.

  Because of this, the MIB recommended revising NASA policy to require a thorough risk assessment for high-priority flight missions, so that the necessary level of government technical surveillance on contract performance could be established. Project plans should clearly define appropriate levels of insight resulting from the risk assessment.

- **Risk Posture Management**

  A rigorous assessment and decision process for managing risk includes ongoing evaluation of NASA's priorities. In DART's case, the lack of adequate risk management contributed to a zero-fault-tolerant design and inadequate testing that resulted in an insufficient collision avoidance system, among other things. Historically, NASA clearly understood and accepted that DART began as a low-cost, high-risk demonstration. As DART's significance changed and it gradually became a highly visible milestone for NASA's high-profile exploration vision, NASA's tolerance for a possible mission failure decreased substantially.

  Because of this, the MIB recommended requiring program and project management committees to regularly review each project's risk level classification in light of changing conditions to ensure continued consistency with the potentially shifting risk tolerance for that project. Decisions to maintain or change a project's classification should be clearly documented.

- **Expert Utilization**

  The MIB noted cases where the DART team failed to fully use the resources of available subject matter experts. Both the insight and peer review processes provided mechanisms for ensuring that adequate technical expertise is supplied to the project.

  The MIB recommended revising NASA policy to clarify that complex, high-priority flight missions be required to use the engineering peer review process. Likewise, the project team should be required to formally address and document its use of the peer reviewers' findings and recommendations.

- **Contractor Review Processes**

  The MIB concluded that internal checks and balances used by DART's prime contractor failed to uncover issues that led to the mishap, such as the undersized spherical envelope surrounding the AVGS range transition waypoint.

  To address this, it recommended that NASA clearly communicate to the contractor its expectations of entrance and exit criteria for standard design and development reviews for high-priority flight projects. Projects should demonstrate the appropriate management rigor in assessing readiness to proceed to the subsequent phase of development.

- **Failure Modes and Effects Analysis (FMEA)**

  The MIB determined that analyses to identify possible hardware/software faults failed to consider a sufficient set of conditions that could lead to the mishap. For example, the analyses focused on the effects of a complete loss of functionality of the navigation system's components, but did not address the impact of a degraded functionality of those same components.

  The MIB recommended that degraded functionality be considered in future analyses, and that those analyses be subject to engineering peer review. In addition, NASA should define the minimum fault tolerance required for spacecraft performing rendezvous missions to protect space assets from collision. Future spacecraft that include autonomous rendezvous, proximity operations, and capture systems should have a collision avoidance sensing capability that is completely independent of the spacecraft's primary navigation sensors. Furthermore, designers for such spacecraft should develop and adhere to a robust, detailed set of requirements for fault detection, isolation, and recovery to prevent a mishap.

  OSMA's endorsement letter states that, "The MIB repeatedly discussed how some of the heritage Pegasus software was used on the DART mission and contributed to the mishap. (This was documented in the report as an intermediate cause to a few contributing factors); however, the MIB's recommendations do not adequately address this." The endorsement letter further states that, "If NASA decides to adopt heritage code, in the future, we (NASA) need to verify that it is appropriate for the mission and fully test it."

Conclusion

In response to the Vision for Space Exploration to the Moon, Mars, and Beyond, NASA has entered a new and exciting period where exploration is a primary objective. Autonomous spacecraft rendezvous, proximity operations, and capture capabilities will continue to be critically important to successful space exploration. As the DART project evolved, its planned mission clearly supported that vision. While DART's transition to a high-visibility project did not proceed as planned, the lessons learned from the mishap will help enable the future development of autonomous capabilities.

Appendix B. GN&C-Related Lessons Learned

Extracted from the NASA LLIS

Subsection	Lesson #	Subject
B.1	0194	Space Shuttle Automatic Landing Capabilities
B.2	0281	Galileo Attitude Control Power on Reset Problem
B.3	0288	Galileo Spacecraft Safing During Star Scanner Calibration
B.4	0310	MO Inertial Reference Loss
B.5	0343	MO Inappropriate Fault Protection Response Following Contingency Mode Entry due to a Postulated Propulsion Subsystem Breach
B.6	0345	MO Attitude Control Fault Protection
B.7	0377	Performance Decrease due to Propulsion Thruster Plume Impingement on the Voyager Spacecraft
B.8	0383	Galileo AACS Computer Memory Access Contention Problem
B.9	0390	Voyager Subsystem Interface Noise Problems
B.10	0400	Spacecraft Structure Dynamical Interaction with Attitude Control
B.11	0403	Thrusters Fired on Launch Pad (1975)
B.12	0409	Voyager Gyro Swap During Launch Phase (1977)
B.13	0422	Particles Generated by Pyrotechnic Events (1967/76)
B.14	0423	Viking Navigation – Unexpected Non-gravitational Acceleration Due to Lander Outgassing (1975)
B.15	0424	Voyager Unbalanced Attitude Control System and Thruster Impingement Effects on Navigation (~1977)
B.16	0593	MPF Avionics and Flight Software Architecture (1997)
B.17	0625	Lewis Spacecraft Mission Failure Investigation Board
B.18	0641	Mars Climate Orbiter MIB – Phase I Report
B.19	0692	Coordinate Systems for Attitude Determination and Control
B.20	0711	Magnetic Field Restraints for Spacecraft Systems and Subsystems
B.21	0726	End-To-End Compatibility and Mission Simulation Testing
B.22	1370	Lessons Learned From Flights of "Off the Shelf" Aviation Navigation Units on the Space Shuttle, GPS
B.23	1480	Provide In-flight Capability to Modify Mission Plans During All Operations (2004)

B-1. Public Lessons Learned Entry: 0194

Lesson Info

- Lesson Number: 0194
- Lesson Date: 04-nov-1992
- Submitting Organization: KSC
- Submitted by: David Pennington

Subject/Title/Topic(s):

Space Shuttle Automatic Landing Capabilities.

Description of Driving Event:

The Space Shuttle system presently includes an autoland system that provides automated guidance capable of navigating the orbiter to the selected landing runway.

The increased duration of space Shuttle flights as part of the Extended Duration Orbiter (EDO) Program has raised the issue of the need to qualify the existing system during actual flights. It also raises the issue of the possible need to fully automate all landing, rollout, and braking functions so the orbiter could be returned safely from orbit without any crew intervention, if necessary.

The existing automated approach guidance system never has been fully flight-tested. The second Space Shuttle flight, STS-2, left the auto mode engaged until the latter part of the team region and demonstrated that the system was capable of returning the vehicle to a flyable energy state from a low-energy state. STS-3 left the system in auto until the commander's scheduled takeover at 125 ft. The system was on energy and trajectory at takeover, but the pilot had difficulty getting "into the loop," and an uncomfortable situation developed. The final several thousand feet of the Shuttle's descent involves relatively complex flare maneuvers with which a pilot might be expected to have difficulty when retaking command.

Lesson(s) Learned:

Significant risk reduction will result if the Shuttle's automatic landing capabilities are fully developed and certified for operational use.

Recommendation(s):

Develop a detailed test of the automatic landing system that will include all functions through touchdown and rollout to wheel stop.

Evidence of Recurrence Control Effectiveness:

N/A

Applicable NASA Enterprise(s):

Human Exploration & Development of Space

Applicable Crosscutting Process(es):

N/A

Additional Key Phrases:

Flight Operations

Flight Equipment

Human Factors

Approval Info:

Approval Date: 06-jun-1994

Approval Name: James G. Kline

Approval Organization:KSC/HEI

Approval Phone Number: 407-867-7614

B-2. Public Lessons Learned Entry: 0281

Lesson Info:

- Lesson Number: 0281
- Lesson Date: 1993-07-12
- Submitting Organization: JPL
- Submitted by: R. F. Collins

Subject:

Galileo Attitude Control Power on Reset Problem

Abstract:

A potentially catastrophic power-on reset (POR) was discovered during testing of the Galileo orbiter. The problem was traced to noise from a capacitive coupling path between flight subsystem ground and support equipment ground. AC ground paths should be testable and should be verified in system interface verification tests. Interface circuits should be analyzed to identify any AC coupling paths between independent ground trees.

Description of Driving Event:

During testing of the Galileo orbiter, an anomaly occurred at infrequent intervals: An unexpected POR event would reinitialize the attitude control subsystem. The POR was recognized as a serious, potentially catastrophic problem, and high priority was given to isolating a cause and verifying a fix. Despite exhaustive investigations and significant design changes to improve noise immunity, the problem continued to occur, infrequently but persistently.

Ultimately, a cause and cure were identified. Although exhaustive test and analysis of ground paths had been carried out, the noise source was identified as a capacitive coupling path between flight subsystem ground and support equipment ground. When spacecraft power surges such as turning on the Traveling Wave Tube Amplifier occurred, the two grounds would experience a transient oscillatory voltage difference of over 7V. The AC Ground Loop fed the transient into the POR sensing circuit and occasionally triggered it. Eliminating the capacitor in the support equipment solved the problem.

Additional Keyword(s): Grounding

Lesson(s) Learned:

AC as well as DC ground paths can be significant in noise coupling between circuits.

Recommendation(s):

1. AC ground paths should be testable and verified in system interface verification tests.
2. Interface circuits should be analyzed to identify any AC coupling paths between independent ground trees.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Energy

Flight Equipment

Ground Equipment

Approval Info:

Approval Date: 1993-10-19

Approval Name: Carol Dumain

Approval Organization: 125-204

Approval Phone Number: 818-354-8242

B-3. Public Lessons Learned Entry: 0288

Lesson Info:

- Lesson Number: 0288
- Lesson Date: 1993-07-13
- Submitting Organization: JPL
- Submitted by: J. O. Blosiu

Subject:

Galileo Spacecraft Safing During Star Scanner Calibration

Abstract:

An unintended in-flight mode change impacted a planned Galileo sequence only because of a hardware failure during the sequence. The spacecraft entered safing, necessitating a difficult recovery process that could have impacted science return had it happened during encounter. When simulating and testing command sequences, assure that the software and hardware states exactly match the expected in-flight states. Any anomaly that changes a fundamental spacecraft state must be scrutinized for potential impacts.

Description of Driving Event:

An attitude and articulation control subsystem (AACS) sequence designed to collect data for calibration of the spacecraft star scanners in the AACS inertial mode (gyroscopes on), was tested on the Galileo test bed simulator.

Prior to the transmission and execution of this calibration sequence on the spacecraft, a star misidentification event caused the AACS to switch from the inertial to the cruise mode (i.e., gyroscopes off).

Because of the importance of getting the calibration data and limited open time in the few weeks before Venus encounter, it was decided to proceed with the star scanner calibration. The mode change was evaluated and not believed to have an effect on the planned sequence.

However, during the execution of the calibration sequence, a spin bearing controller instability occurred due to an unexpected incompatibility between the mode and AACS software. This caused a series of hardware swaps within the AACS, ultimately causing the spacecraft to go into safing. A subsequent test on the Galileo test bed simulator duplicated the spacecraft response.

This event occurred 25 days before Venus encounter, and the difficult recovery process from safing took three weeks. Had this anomaly occurred closer to the encounter, significant impact on science data return could have resulted.

Reference(s): PFR #52608

Lesson(s) Learned:

1. Test bed simulators provide a valuable tool for analyzing/verifying spacecraft operations and anomalies.
2. Spacecraft mode changes caused by in-flight anomalies can affect subsequent planned activity sequences.

Recommendation(s):

1. When simulating and testing command sequences, care must be taken to guarantee that the software and hardware states used during the test exactly match the software and hardware states expected in flight.
2. Whenever a spacecraft anomaly changes any of the fundamental spacecraft states, all subsequent activities must be scrutinized for potential impacts.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

Science

Additional Key Phrase(s):

Flight Operations

Spacecraft

Test & Verification

Approval Info:

Approval Date: 1993-10-19

Approval Name: Carol Dumain

Approval Organization: 125-204

Approval Phone Number: 818-354-8242

B-4. Public Lessons Learned Entry: 0310

Lesson Info:

- Lesson Number: 0310
- Lesson Date: 1994-03-03
- Submitting Organization: JPL
- Submitted by: G. T. Chien / J. O. Blosiu

Subject:

Mars Observer Inertial Reference Loss

Abstract:

MO experienced inertial reference loss on several occasions during its cruise to Mars. These incidents were due to the lack of a detailed code walk-through and to use of gyroscope noise values, obtained from in-house test, that were more optimistic than the manufacturer's specifications. Do not depend on hardware performance being better than the manufacturer's specification. Perform detailed code walk-through of critical software modules. Pay special attention to inherited critical software. Design the flight computer and software to permit necessary changes in flight.

Description of Driving Event:

MO experienced inertial reference loss on several occasions during its cruise to Mars. Two classes of inertial reference loss have been observed:

1. In early January 1993, the FSW was unable to identify any star that transited the celestial sensor assembly field of view. The unidentified stars count exceeded the "loss logic limit," and the fault protection software commanded the spacecraft to the Sun coning attitude contingency mode. This occurred three times before a temporary software script to widen the star identification tolerance was uplinked in order to artificially increase the attitude uncertainties, or covariances, used by the software. Design flexibility of the fight computer and software allowed the software patch to be easily performed. It was suspected that the cause was due to the use of the more optimistic gyroscope noise parameters and values obtained from the in-house test results rather than the manufacturer's specifications. Recovery time: 3 days per occurrence.
2. During April and May 1993, three more incidents caused the spacecraft to declare inertial reference loss when the Sun monitor ephemeris test, which compares the expected new position with the measured positions, was violated. An algorithm error in the inherited FSW caused the spacecraft attitude to be incorrectly estimated under certain conditions. A similar problem occurred on the Defense Meteorological Satellite Program (DMSP), an Earth-orbiting spacecraft built by the same contractor, that was using the same flight software. This algorithm error puts the spacecraft in additional jeopardy when the attitude covariances are large. Since the script that was intended to prevent the January incidents increased the covariances, the script acted as a catalyst for the three April/May anomalies. The data review indicated that no detailed code walk-through was performed on the software patch that widened the star identification tolerance. Recovery time: 5 days per occurrence.

Additional Keyword(s): Attitude Determination, Star Scanner

Lesson(s) Learned:

1. Hardware performance based on in-house tests are not substitutes for manufacturer specifications for components whose performance varies (i.e., degrades) over mission life (e.g., gyroscopes).
2. Non-performance of detailed code walk-through for critical software could have serious effects on spacecraft operation. The covariance program bugs in the FSW should have been caught even before testing of the code.
3. Inherited software designed for Earth-orbiting satellites may not be directly applicable to interplanetary spacecraft missions.
4. Design flexibility of the flight computer and software is critical to the ability to uplink software patches for the correction of unexpected in-flight spacecraft anomalies.

Recommendation(s):

1. Do not depend on hardware performance being better than the manufacturer's specification.
2. Perform detailed code walk-through of critical software modules, particularly of FSW patches.
3. Special attention should be paid to flight-critical software performance inherited from previous applications. Prior anomalies must be addressed.
4. Allow sufficient flexibility in the flight computer and software to permit necessary changes in flight.

Evidence of Recurrence Control Effectiveness: N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Computers

Flight Equipment

Software

Test & Verification

B-5. Public Lessons Learned Entry: 0343

Lesson Info:

- Lesson Number: 0343
- Lesson Date: 1994-09-29
- Submitting Organization: JPL
- Submitted by: G.T. Chen / J.O. Blosiu

Subject:

Mars Observer Inappropriate Fault Protection Response Following Contingency Mode Entry Due to a Postulated Propulsion Subsystem Breach

Abstract:

Following the loss of the MO spacecraft, simulations showed that a postulated propellant breach would have caused angular accelerations that could have inhibited downlink and caused multi-axis gyroscope saturation. In this case, fault protection features of FSW would have inhibited all momentum unloading and prevented the stabilization of the spacecraft.

Ensure that fault protection takes proper action regardless of spacecraft state. Fault responses should not be allowed to interrupt critical activities.

Description of Driving Event:

Verification Test Laboratory simulations of the MO spacecraft spin-up were performed to simulate a postulated propellant subsystem breach. The results indicated that even moderately low angular accelerations caused by the postulated propulsion subsystem breach could have triggered a contingency mode entry that interfered with the Radio Power Amplifier (RPA) turn-on cycle. Under these circumstances, contingency mode entry would have inhibited downlink until a ground command was sent. In contingency mode, fault protection was not capable of properly configuring the telecommunication subsystem to re-establish downlink autonomously. Contingency mode was a stable state, and FSW could have stayed in this mode indefinitely.

This angular acceleration level would have caused multi-axis gyroscope saturation. If multi-axis gyroscope saturation was entered, FSW would have inhibited all momentum unloading, thus preventing the stabilization of the spacecraft. Assuming sunlight on the array 33% of the time, battery depletion could be expected within 4.5 +/- 0.5 hours (sooner for even less favorable Sun angle). The ground commands to re-activate RPA were not issued until about 4.5 hours after propellant pressurization since spacecraft autonomy was assumed capable to solve the issue. By the time these ground commands were issued, the batteries most likely would have been depleted.

The above postulated sequence of mishaps could have been the cause of MO loss of signal.

Additional Keyword(s): Sequence Interaction, Attitude Control

Reference(s):

1. Mars Observer Loss of Signal: Special Review Board Final Report: JPL Pub. 93-28
2. Mars Observer Fault Protection Response in High Spacecraft Spin Rates, IOM MOS 94-159, 06/17/94, G. T. Chen to D. E. Bernard.

Lesson(s) Learned:

Inappropriate fault protection actions can be as hazardous as the failure the system was designed to protect against.

Recommendation(s):

1. It is imperative that spacecraft designers consider the consequences of anomalies at all mission phases and ensure fault protection takes proper action regardless of spacecraft state.
2. Fault responses should not be allowed to interrupt critical activities unless they have the ability to assure completion of these activities. Final, stable fault protection modes (such as contingency mode) should autonomously assure communications.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Hardware

Safety & Mission Assurance

Software

Spacecraft

B-6. Public Lessons Learned Entry: 0345

Lesson Info:

- Lesson Number: 0345
- Lesson Date: 1994-10-10
- Submitting Organization: JPL
- Submitted by: D.E. Bernard / J.O. Blosiu

Subject:

Mars Observer Attitude Control Fault Protection

Abstract:

From the analyses performed after the MO mission failure, it became apparent that the MO fault protection suffered from a lack of top-down system engineering design approach. Most fault protection was in the category of low-level redundancy management. It was also determined that the fault protection software was never tested on the spacecraft before launch. Design fault protection to detect and respond to excessive attitude control errors, use RCS thrusters to control excessive attitude control errors, and always test fault protection software on the flight spacecraft before launch.

Description of Driving Event:

No AACS or fault protection failure was identified as a likely direct cause of the MO mission failure. Nevertheless, modification to the MO AACS and fault protection design could have: a) stabilized the spacecraft and reestablished communications in the postulated pressurant line burst scenario, and b) increased the likelihood of stabilizing the spacecraft after a power-on-reset in the electronic part latch-up scenario.

By analyzing MO software algorithms and documentation, as well as performing verification test laboratory simulations of the spacecraft, it became apparent that the MO fault protection suffered from a lack of top-down system engineering design approach. Most fault protection was in the category of low-level redundancy management. It was also determined that the MO fault protection software was never tested on the flight spacecraft before launch.

Furthermore, it was determined that in case of excessive attitude control errors, the spacecraft would not be stabilized by the RCS thrusters. No RCS thruster control algorithms were present in the software code, thus there was no functional back-up to the RWAs for attitude control. If the RCS thrusters were used directly for control, they could have prevented a spin-up for most pressurant line burst scenarios.

Additional Keyword(s): Software Testing

Reference(s):

1. Fault Protection Lessons Learned from Mars Observer Loss of Signal Briefing to Division 34 Staff, Douglas E. Bernard 07/20/94.
2. Mars Observer Loss of Signal: Special Review Board Final Report: JPL Pub. 93-28.

Lesson(s) Learned:

1. MO fault protection did not detect and respond to excessive attitude control errors.
2. RCS thrusters were not used to correct excessive attitude control errors.
3. Fault protection software was never tested on the flight spacecraft before launch.

Recommendation(s):

1. Design fault protection to detect and respond to excessive attitude control errors.
2. Use RCS thrusters to control excessive attitude control errors.
3. Always test fault protection software on the flight spacecraft before launch.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Safety & Mission Assurance

Spacecraft

Test & Verification

Approval Info:

Approval Date: 1994-10-20

Approval Name: Marilyn Platt

Approval Organization: 186-120

Approval Phone Number: 818-354-0880

B-7. Public Lessons Learned Entry: 0377

Lesson Info:

- Lesson Number: 0377
- Lesson Date: 1995-01-31
- Submitting Organization: JPL
- Submitted by: B. Wagoner / J.A. Bryant

Subject:

Performance Decrease Due to Propulsion Thruster Plume Impingement on the Voyager Spacecraft

Abstract:

A 21% shortfall in Voyager's velocity change was suspected to be due to exhaust plume impingement. Due to the complexity of spacecraft/thruster configurations, additional care must be taken in the development and utilization of spacecraft and plume models. Analysis should be conducted on early and final designs.

Description of Driving Event:

The initial Voyager Spacecraft TCM delivered approximately 21 percent less velocity change than predicted. Since the spacecraft telemetry indicated that pointing accuracy, thruster performance, and spacecraft equipment all were normal, it was suspected that the degradation was due to exhaust plume impingement effects.

Subsequent analysis indicated that pre-flight models underestimated the effects of plume impingement due to over-simplified geometry models and inadequate characterization of rarefied gas dynamics flow fields.

Reference(s): PFR #41003.

Lesson(s) Learned:

Rocket engine plume effects can vary dramatically as a function of thruster type, location, and operating conditions, and interaction of plumes with the spacecraft structure and/or other subsystems can have a substantial impact on spacecraft performance.

Recommendation(s):

1. Due to the complexity of spacecraft/thruster configurations, additional care must be taken in the development and utilization of spacecraft and plume models.
2. Analysis should be conducted on early and final designs as part of the normal design team activity.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Flight Equipment

Spacecraft

B-8. Public Lessons Learned Entry: 0383

Lesson Info:

- Lesson Number: 0383
- Lesson Date: 1995-02-15
- Submitting Organization: JPL
- Submitted by: J.C. Marr / P.D. Lisman

Subject:

Galileo AACS Computer Memory Access Contention Problem

Abstract:

Galileo AACS checksum errors resulted from bus contentions caused by noise from electromagnetic coupling within the AACS intra-subsystem harness. Recommendations included simulations and other methods for thoroughly characterizing the electrical performance of cables.

Description of Driving Event:

During system level testing, repeated AACS checksum errors occurred without the presence of actual memory content errors (i.e., miscompares). These checksum errors occurred only when in one of the four possible CPU-memory configurations and only when the Command and Data Subsystem (CDS) was accessing the off-line memory. Extensive troubleshooting on the spacecraft showed that the anomalous checksum errors were being caused by both AACS memories placing data on the data bus at the same time (i.e., bus contention).

After further subsystem testing and analysis, subsystem engineers determined that the bus contentions were caused by electromagnetic coupling within the AACS intra-subsystem harness while simultaneously accessing both AACS memories. Specifically, data being placed on the data bus by the on-line memory induced noise on the address lines which caused the off-line memory to turn on its data line drivers during an off-line CDS direct memory access cycle.

The noise coupling between the address and data lines occurred in spite of AACS bay harness design which was in compliance with JPL and Galileo design standards. Further, the limited-fidelity CDS simulator used during subsystem testing prevented finding the problem prior to spacecraft integration.

Additional Keyword(s): Circuit Noise

Reference(s): PFR #44836.

Lesson(s) Learned:

1. Design to JPL or project standards is not always sufficient to ensure adequate performance of subsystem cabling. In this era of rapid technological change, design standards used successfully in the past may not be sufficient to preclude problems in the present.
2. Simulators of subsystem interfaces with other subsystems may not always provide adequate performance assessment for the spacecraft environment.
3. Limited fidelity of simulators used during subsystem testing can prevent diagnosis of subsystem problems prior to spacecraft integration.

Recommendation(s):

1. The cognizant engineer must fully consider the electrical performance of the cable in his specific subsystem application.
2. The subsystem impact of simulator limitations should be thoroughly understood and documented. Additionally, testing with integrated breadboards instead of simulators should be encouraged.
3. Subsystem equipment must be adequately tested on the spacecraft in all redundant configurations to ensure that equipment configuration dependent problems are found.
4. Noise on intra-subsystem cabling must be thoroughly investigated as to cause and effects as early as possible in subsystem testing.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Hardware

Test & Verification

B-9. Public Lessons Learned Entry: 0390

Lesson Info:

- Lesson Number: 0390
- Lesson Date: 1995-03-21
- Submitting Organization: JPL
- Submitted by: B. Larman

Subject:

Voyager Subsystem Interface Noise Problems

Abstract:

Problems due to waveform irregularities and the resultant induced noise on the Voyager Spacecraft system interfaces were not validated until 500 hours of system testing had been completed. Lessons involve the need for early system tests to determine subsystem compatibility and design requirements for electrical noise and transients, and extensive interface testing under flight-like conditions.

Description of Driving Event:

Problems due to waveform irregularities and the resultant induced noise on the Voyager Spacecraft system interfaces were not validated until after in excess of 500 hours of system testing had been completed. The problem manifested itself in the following two ways:

1. A digital, coded interface design was utilized on the Voyager Spacecraft for transferring command data between the Computer Command Subsystem (CCS) and the power subsystem. This interface, under certain spacecraft system loading configurations with the support equipment disconnected, resulted in several cases of either “no response” or “incorrect response” to commands. The problem was traced to the 2.4 kHz power subsystem waveform transitions (variable with system load configuration) coupling into the command circuits via its circuit returns causing spurious clock pulses.
2. A related but not identical problem occurred on the CCS to the AACS command interface. In this case, waveform transition irregularities of the 2.4 kHz clock signal (again, variable with system load configuration) could, under certain conditions, result in trigger circuits interpreting these irregularities as clock pulses.

To correct these problems required circuit modifications to all affected subsystems which entailed extensive regression testing. Details can be found in Voyager PFR 39802 and IOM 3132-76-179.

Lesson(s) Learned:

1. Early testing of subsystem compatibility can detect problems and avoid extensive subsystem modifications.
2. Waveform transition irregularities and resultant induced noise problems on spacecraft system interfaces, if not validated prior to system testing of flight hardware, can require circuit modifications to affected subsystems and extensive regression testing.

3. It is virtually impossible to simulate the real noise environment of the complete spacecraft in the subsystem test facility.

Recommendation(s):

1. System tests to determine subsystem compatibility should begin as early as possible using prototype or breadboard hardware. Testing of the system without the subsystem support equipment cables attached should also be conducted as early as possible. It has been found that these cables can alter the flight configuration noise environment considerably.
2. Critical system-level interface electrical noise and transient design requirements should be generated early by systems engineering. These should be reviewed and understood by the subsystem design engineers prior to circuit design. Critical subsystems interface circuit design should be reviewed by the system engineer prior to implementation.
3. It is essential that early and extensive interface testing be conducted with as many system loading and flight-like conditions as possible. Where noise immunity is critical, injection of noise on the signal lines during subsystem tests may be necessary to demonstrate adequate margins.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Spacecraft

Test & Verification

B-10. Public Lessons Learned Entry: 0400

Lesson Info:

- Lesson Number: 0400
- Lesson Date: 1995-06-08
- Submitting Organization: JPL
- Submitted by: J. Langmaier

Subject:

Spacecraft Structure Dynamical Interaction with Attitude Control

Abstract:

As Mariner 10 approached Venus encounter, an uncontrolled oscillation occurred due to spacecraft structural interaction with the ACS. The result was a severe consumption of control gas that would have caused failure of the mission had it continued. The recommendations center on design and operational measures to cope with subtle and complex dynamical interactions between the spacecraft structure and the ACS.

Description of Driving Event:

As Mariner 10 (MVM'73) was nearing encounter with Venus, an uncontrolled oscillation occurred due to spacecraft structural interaction with the ACS. The problem was first detected during a platform calibration sequence, which required a series of roll turns using roll gyroscope inertial control and science scan platform motion. The result was a severe consumption of control gas, which would have caused mission failure had it continued.

The oscillation was due to a control instability exciting a structural mode of the spacecraft. The primary cause of the resonance was attributed to solar panel flexibility.

Additional Keyword(s): Flexible Body Analysis

Reference(s): PFR #5024.

Lesson(s) Learned:

Spacecraft structural dynamical interactions with the ACS can be very subtle and complex.

Recommendation(s):

1. During the spacecraft design phase, consideration should be given to:
   a. Increasing the amount of analysis on and simulation of structural/control interactions.
   b. Placing additional or tighter controls on key parameters at interfaces between structures and attitude control.
   c. Establishing procedures for communicating key parameter data between subsystem engineers and analysts, initially and when changed.
2. In situations where there is significant uncertainty in simulations, models, or analysis results, the spacecraft subsystem software should be designed to accommodate changes late in the development, test, and post-launch periods. Techniques such as modular design and parameter tables vs. hard coding should be considered.

3. The capability to cope with this type of anomaly, by analysis and simulation, should be maintained throughout the mission.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Flight Equipment

Hardware

Software

Spacecraft

Approval Info:

Approval Date: 1996-01-26

Approval Name: Carol Dumain

Approval Organization: 125-204

Approval Phone Number: 818-354-8242

B-11. Public Lessons Learned Entry: 0403

Lesson Info:

- Lesson Number: 0403
- Lesson Date: 1996-04-26
- Submitting Organization: JPL
- Submitted by: J.A. Roberts

Subject:

Thrusters Fired on Launch Pad (1975)

Abstract:

Inadvertent commanding of the safing sequence while Voyager 2 was still on the launch pad enabled the RCS thrusters. The thrusters fired in an attempt to compensate for the Earth's rotation, resulting in a significant loss of attitude control gas. When command sequences intended to be exercised only in the event of abnormal spacecraft activity are stored onboard, consider the consequences of their activation during system test or the pre-launch phases.

Description of Driving Event:

(Relevant Historical Lesson(s) Learned)

On VO'75, a launch pad problem developed involving the FSW program and the Reaction Control System thrusters. The flight software, intended for use only after launch, contained within it a "safing sequence." The intent of the safing sequence was to automatically place the spacecraft in a safe state should some anomaly be detected. The safing sequence included commands to enable the RCS and its thrusters.

In spite of procedural safeguards, a problem developed which inadvertently resulted in the issuance of the safing sequence while VO-2 was still on the launch pad. This, in turn, enabled the RCS thrusters. The ACS then sensed the Earth's rotation, causing the RCS thrusters to fire in an attempt to compensate. Thruster firing continued until disabled by the test team, resulting in a significant loss of N2 attitude control gas. The launch was conducted without replacing the lost gas, rather than take the spacecraft down off the launch vehicle for replenishment. The safing sequence was also inadvertently issued several times during system test, but no adverse consequences resulted.

Additional Keyword(s): Ground Operations, Pre-Launch Constraints

Reference(s): VO'75 P/FR #34869

Lesson(s) Learned:

When command sequences are stored on the spacecraft and intended to be exercised only in the event of abnormal spacecraft activity, the consequences of their being issued during the system test or pre-launch phases should be considered.

Recommendation(s):

Had the ability of the safing sequence to enable the thrusters been constrained in some manner until after launch, for example, the VO'75 problem would not have occurred.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Ground Operations

Software

Spacecraft

B-12. Public Lessons Learned Entry: 0409

Lesson Info:

- Lesson Number: 0409
- Lesson Date: 1996-06-24
- Submitting Organization: JPL
- Submitted by: J.A. Roberts

Subject:

Voyager Gyroscope Swap During Launch Phase (1977)

Abstract:

Because the VO- 2 failure protection logic was unnecessarily enabled during launch, transient gyroscope outputs triggered a series of alarming “gyro swaps.” Careful attention should be given to preclude the possibility of spurious inputs triggering unwanted events when the protection logic is enabled.

Description of Driving Event:

(Relevant Historical Lesson(s) Learned)

VO- 2 experienced gyroscope control problems during launch because its failure protection logic was enabled. Attitude control required data about all three spacecraft axes: roll (R), pitch (P), and yaw (Y). The three 2-axis gyroscopes on Voyager provided data, respectively, about the R-P, P-Y, and Y-R axes. Thus any two gyroscopes together provided the required three-axis data, plus a fourth, redundant set of data about an axis common to both gyroscopes. The third gyroscope acted as backup. The gyroscopes, not needed until just before separation from the Titan/Centaur, were left “on” and thus warmed up during launch to ensure immediate readiness.

The failure protection logic, also left enabled during launch, sensed failure by comparing the output of the axis common to both controlling gyroscopes. If not equal, the back-up replaced one controlling gyroscope. If still not equal, the gyroscopes were switched again. Continued inequality among all possible gyroscope pairs caused the logic to look elsewhere for the problem.

It was understood a priority that the gyroscope output would saturate during launch, and that this saturation output would be at equal limiting values, ensuring a valid logic comparison. Instead, however, the output oscillated significantly, causing a miscomparison. Telemetry then indicated the series of “gyro swaps” as the failure protection logic attempted unsuccessfully to pair gyroscopes having equal output. This led Mission Operations to suspect a major failure on VO-2.

Lesson(s) Learned:

It is suggested that failure protection logic be enabled only when the protected components or subsystems are required for spacecraft operation. Careful attention should be given to preclude the possibility of spurious inputs triggering unwanted events when the protection logic is enabled.

Recommendation(s):

The gyroscopes were not used for attitude control until just before separation from the Centaur. Thus, the failure protection logic function was not needed until that time. To prevent a recurrence of the VO-2 experience, the failure protection logic was disabled on Voyager 1[6] during periods of launch vehicle thrusting.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Flight Equipment

Spacecraft

[6] Voyager 1 was launched after Voyager 2.

B-13. Public Lessons Learned Entry: 0422

Lesson Info:

- Lesson Number: 0422
- Lesson Date: 1996-07-10
- Submitting Organization: JPL
- Submitted by: J.A. Roberts

Subject:

Particles Generated by Pyrotechnic Events (1967/76)

Abstract:

Following a Viking Orbiter pyrotechnic-actuated event, debris was viewed by the star tracker as numerous bright objects, initiating a command to change the spacecraft roll position. During and following a pyrotechnic event, place the spacecraft in roll inertial and disable any Canopus-loss fault protection software.

Description of Driving Event:

(Relevant Historical Lesson(s) Learned)

At the time of Mariner 6 scan platform unlatching, which was effected by firing a pyrotechnic squib, several bright objects were seen by the Canopus tracker. This caused the tracker to lose lock on Canopus, causing a roll search to be initiated.

For 25 minutes following the first opening of the VO-1 propellant pressurant supply (a pyrotechnic-actuated event), the spacecraft roll axis was commanded to roll inertial hold and the Canopus-loss fault protection software was disabled. During the first part of this period, numerous bright objects were seen by the Canopus tracker. Within a few minutes after completion of the inertial hold period, another bright particle was seen by the tracker, this time causing the spacecraft roll position to change and the on-board software to execute the Canopus-loss fault protection response.

Additional Keyword(s): Attitude Control, Science Viewing

Lesson(s) Learned:

Always take the precaution of placing the spacecraft in roll inertial and disabling any Canopus-loss fault protection software at and following a pyrotechnic event. At these times particles are shocked loose from parts of the spacecraft, from whence they drift through the Canopus tracker field of view.

Recommendation(s):

Provide at least an hour’s protection period following these events before returning the spacecraft to normal roll control.

Bright objects resulting from a pyro event may also adversely affect other devices such as science instruments. A one-hour delay in operating these devices should be considered.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Energetic Materials – Explosive/Propellant/Pyrotechnic

Flight Operations

Spacecraft

B-14. Public Lessons Learned Entry: 0423

Lesson Info:

- Lesson Number: 0423
- Lesson Date: 1996-07-10
- Submitting Organization: JPL
- Submitted by: J.A. Roberts

Subject:

Viking Navigation – Unexpected Non-Gravitational Acceleration Due to Lander Outgassing (1975)

Abstract:

Immediately after the launch of Viking I, large and unexpected non-gravitational accelerations were detected and attributed to outgassing from porous materials (e.g., parachute, blankets) in the lander. A midcourse correction made to preclude large targeting errors upon Mars Encounter.

Every spacecraft design should be reviewed for its potential for outgassing (and its impact on the navigation strategy and the spacecraft) throughout flight.

Description of Driving Event:

(Relevant Historical Lesson(s) Learned)

Immediately after the launch of Viking I, large and unexpected non-gravitational accelerations were seen when the Doppler observations of the spacecraft were processed for orbit determination. These perturbations to the spacecraft dynamics were confirmed by observations of the attitude-control limit-cycle motion. Spacecraft team analysis identified the cause as the venting of outgassing products from porous materials (e.g., parachute, blankets) in the lander. There was considerable uncertainty in the expected duration of the effect. This uncertainty raised the possibility of large targeting errors at Mars; consequently, the effect was included in the design of the midcourse correction made shortly after departure from Earth. The effect appeared to cease 1 to 2 months after launch, and did not in fact significantly increase targeting errors. The same effect was observed on Viking II.

Lesson(s) Learned:

Every spacecraft design should be reviewed for outgassing potential at any time during flight.

Recommendation(s):

The magnitude of the resulting non-gravitational accelerations should be estimated and compared with the navigation requirements on non-gravitational accelerations. If these requirements are exceeded, re-design of the navigation strategy and/or the spacecraft may be required.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Flight Equipment

Parts Materials & Processes

Spacecraft

B-15. Public Lessons Learned Entry: 0424

Lesson Info:

- Lesson Number: 0424
- Lesson Date: 1996-07-10
- Submitting Organization: JPL
- Submitted by: J.A. Roberts

Subject:

Voyager Unbalanced Attitude Control System and Thruster Impingement Effects on Navigation (~1977)

Abstract:

Shortly after the Voyager launch, unexpected dynamic effects necessitated additional orbit determination analysis, testing, and modeling to ensure an accurate trajectory. Perform careful coordinated pre-flight analysis to determine the impact of such effects as torques induced by solar pressure and gas impingement on the spacecraft structure. Design and test to avoid impingement problems.

Description of Driving Event:

(Relevant Historical Lesson(s) Learned)

Shortly after Voyager launch, unexpected translational velocity increments and large non-gravitational acceleration effects were observed in the orbit-determination processing of tracking data. These velocity increments and accelerations were traced to the unbalanced translational accelerations produced by the attitude control system, its response to torques induced by solar pressure, and to the impingement of gas from the pitch thrusters onto other parts of the spacecraft structure. The magnitude of these dynamic effects required that they be modeled in the orbit determination process throughout the flight. This involved additional orbit determination processing and analysis, and necessitated a new operational interface between the Spacecraft Team and Navigation Team. A special in-flight impingement test was performed to provide data for modeling. The pre-flight analysis to recognize or predict the effects and uncertainties from both the unbalanced thrusters and the impingement was inadequate. The result was incomplete flight operations planning by both the Spacecraft and Navigation Teams.

Additional Keyword(s): Trajectory Accuracy

Lesson(s) Learned:

Orbit determination complexity is increased significantly when translational accelerations from the attitude control system must be accounted for.

Recommendation(s):

Careful coordinated pre-flight analysis by both the Navigation and Spacecraft areas is needed to estimate the size and uncertainties of these effects, establish the necessary operational interfaces, and estimate the scope of the operations task. Spacecraft designs must be reviewed with an eye to avoiding impingement problems. If impingement is suspected, a test similar to the Voyager impingement test should be planned and executed early in the flight.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Hardware

Spacecraft

Approval Info:

Approval Date: 1996-07-10

Approval Name: Carol Dumain

Approval Organization: JPL

Approval Phone Number: 818-354-8242

B-16. Public Lessons Learned Entry: 0593

Lesson Info:

- Lesson Number: 0593
- Lesson Date: 1998-06-18
- Submitting Organization: JPL
- Submitted by: G. Reeves/D. Oberhettinger

Subject:

Mars Pathfinder Avionics and Flight Software Architecture (1997)

Abstract:

The MPF avionics and FSW development effort focused on producing a software architecture that would contribute to lower operations cost and minimize overall project cost. This lesson summarizes MPF success factors, including use of an extra-powerful flight computer and a standardized backplane and bus.

Description of Driving Event:

The MPF avionics and FSW development effort focused on producing a software architecture that would contribute to lower operations cost and minimize the overall project cost.

Additional Keyword(s): Software Life Cycle, Life Cycle Cost, Concurrent Engineering

Reference(s):

1. Glenn Reeves, “Mars Pathfinder Flight Software Lessons Learned,” April 28, 1997.
2. “Mars Pathfinder Flight Software Development Process,” JPL Lesson Learned No.10-105, June 4, 1998.

Lesson(s) Learned:

1. Use of a powerful computer (20 MIPS) with large memory for margin management provided flexibility in software development for MPF.
2. Consider use of a commercial standard backplane (e.g., VME) and avionics standard bus (such as MIL-STD-1553) to allow the fast development of realistic test environments using commercial hardware and software.
3. The early MPF risk assessments prompted the use of an essentially single string avionics design, which resulted in a great reduction in the complexity of the software.
4. A multitasking execution model permits parallel development of separate modules and is supported by a variety of commercial products.
5. Purchase a commercial operating system (kernel) rather than developing one in house.
6. Select a mature flexible implementation language, with mature development tools, such as the C language.
7. The MPF project combined the CDS and ACS hardware and software functions in one processor. This greatly simplified hardware design, ground and FSW design, system implementation, and integration and test.

8. Consider using software system analysts to directly produce flight code, instead of just writing software specifications and handing them to a FSW team to code.

Recommendation(s):

See Lessons Learned

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

N/A

Additional Key Phrase(s):

Administration/Organization

Computers

Risk Management/Assessment

Software

Approval Info:

Approval Date: 1998-06-25

Approval Name: Carol Dumain

Approval Organization: 125-204

Approval Phone Number: 818-354-8242

B-17. Public Lessons Learned Entry: 0625

Lesson Info:

- Lesson Number: 0625
- Lesson Date: 1998-02-12
- Submitting Organization: GSFC
- Submitted by: Charles Vanek

Subject:

Lewis Spacecraft Mission FIB

Description of Driving Event:

The Lewis Spacecraft was procured by NASA via a 1994 contract with TRW Inc., and launched on August 23, 1997. Contact with the spacecraft was subsequently lost on August 26, 1997. The spacecraft re-entered the atmosphere and was destroyed on September 28, 1997.

The Lewis Spacecraft Mission FIB was established to gather and analyze information and determine the facts as to the actual or probable cause(s) of the Lewis Spacecraft Mission Failure. The FIB was also tasked to review and assess the FBC Lewis spacecraft acquisition and management processes used by NASA and the contractor to determine whether they may have contributed to the failure. The investigation process used by the board was to individually interview all persons believed to have had a substantial involvement in the Lewis spacecraft acquisition, development, management, launch, operations and the events that may have led to the eventual loss. These interviews were aimed at not only understanding the facts as they occurred but also at understanding the individual perceptions that may have been instrumental in the decisions and judgments as made on this Program.

Lesson(s) Learned:

The Board found that the loss of the Lewis Spacecraft was the direct result of an implementation of a technically flawed Safe Mode in the Attitude Control System. This error was made fatal to the spacecraft by reliance on that Safe Mode by the on orbit operations team and by the failure to adequately monitor spacecraft health and safety during the critical initial mission phase.

The Board also discovered numerous other factors that contributed to the environment that allowed the direct causes to occur. While the direct causes were the most visible reasons for the failure, the Board believes that the indirect causes were also very significant contributors. Many of these factors can be attributed to a lack of a mutual understanding between the contractor and the Government as to what is meant by FBC. These indirect contributors are to be taken in the context of implementing a program in the FBC mode:

- Requirement changes without adequate resource adjustment
- Cost and schedule pressures
- Program Office move
- Inadequate ground station availability for initial operations
- Frequent key personnel changes
- Inadequate engineering discipline
- Inadequate management discipline

The Board strongly endorses the concept of "Faster, Better, Cheaper" in space programs and believes that this paradigm can be successfully implemented with sound engineering and attentive and effective management. However, the role changes for government and industry are significant and must be acknowledged, planned for, and maintained throughout the program. Since these roles are fundamental changes in how business is conducted, they must be recognized by all team members and behaviors adjusted at all levels. The board observed an attempt during the early phase of the Lewis Program to work in a FBC culture, but as the program progressed the philosophy changed to business as usual, with dedicated engineers working long hours using standard processes to meet a short schedule and skipping typical government oversight functions.

Recommendation(s):

Based on observations from the Lewis Program, the FIB offers the following recommendations to enhance mission success in future programs performed under this new paradigm:

Balance Realistic Expectations of FBC

Meaningful trade space must be provided along with clearly articulated priorities. Price realism at the outset is essential, and any mid-program change must be implemented with adequate adjustments in cost and schedule. This is especially important in a program that has been implemented with minimal reserves.

Establish Well-Understood Roles and Responsibilities

The Government and the contractor must be clear on the mutual roles and responsibilities of all parties, including the level of reviews and what is required of each side and each participant in the Integrated Product Development Team.

Adopt Formal Risk Management Practices

FBC methods are inherently more risk-prone and must have their risks actively managed. Disciplined technical risk management must be integrated into the program during planning and must include formal methods for identifying, monitoring, and mitigating risks throughout the program. Individually small, but unmitigated, risks on Lewis produced an unpredicted major effect in the aggregate.

Formalize and Implement Independent Technical Reviews

The internal Lewis reviews did not include an adequate action response and closure system and may have received inadequate attention from the contractor's functional organizations. The government has the responsibility to ensure that competent and independent reviews are performed by the government, the contractor, or both.

Establish and Maintain Effective Communications

A breakdown of communications and a lack of understanding contributed to wrong decisions being made on the Lewis program. For example, the decision to operate the early on-orbit mission with only a single shift of ground control crew was not clearly communicated to senior TRW or NASA management. The board believes that, especially in a FBC program, these working relationships are the key to successful program implementation.

Although this report necessarily focused on what went wrong with the Lewis Program, much also went right due to the skill, hard work, and dedication of many people. In fact, these people completely designed, constructed, assembled, integrated, and tested a complex space system within the two-year goal and probably came very close to mission success.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

Science

Additional Key Phrase(s):

Administration/Organization

Communication Systems

Computers

Financial Management

Flight Operations

Flight Equipment

Ground Operations

Hardware

Information Technology/Systems

Mishap Reporting

Risk Management/Assessment

Software

Spacecraft

B-18. Public Lessons Learned Entry: 0641

Lesson Info:

- Lesson Number: 0641
- Lesson Date: 1999-12-01
- Submitting Organization: HQ
- Submitted by: Pete Rutledge

Subject:

Mars Climate Orbiter MIB – Phase I Report

Description of Driving Event:

Mars Climate Orbiter Spacecraft

The MCO Mission objective was to orbit Mars as the first interplanetary weather satellite and provide a communications relay for the MPL, which was due to reach Mars in December 1999. The MCO was launched on December 11, 1998, and was lost sometime following the spacecraft's entry into Mars occultation during the MOI maneuver. The spacecraft's carrier signal was last seen at approximately 09:04:52 UTC on Thursday, September 23, 1999.

Lesson(s) Learned:

The MCO MIB has determined that the root cause for the loss of the MCO spacecraft was the failure to use metric units in the coding of a ground software file used in trajectory models. Specifically, thruster performance data in English units instead of metric units was used in the software application code titled SM_FORCES (Small Forces). A file called AMD contained the output data from the SM_FORCES software. The data in the AMD file was required to be in metric units per existing software interface documentation, and the trajectory modelers assumed the data was provided in metric units per the requirements.

During the 9-month journey from Earth to Mars, propulsion maneuvers were periodically performed to remove angular momentum buildup in the on-board reaction wheels (flywheels). These AMD events occurred 10-14 times more often than was expected by the operations navigation team. This was because the MCO solar array was asymmetrical relative to the spacecraft body as compared to MGS, which had symmetrical solar arrays. This asymmetric

effect significantly increased the solar pressure-induced momentum buildup on the spacecraft. The increased AMD events, coupled with the fact that the angular momentum (impulse) data was in English, rather than metric, units, resulted in small errors being introduced in the trajectory estimate over the course of the 9-month journey. At the time of Mars insertion, the spacecraft trajectory was approximately 170 kilometers lower than planned. As a result, MCO either was destroyed in the atmosphere or re-entered heliocentric space after leaving Mars' atmosphere.

The MIB recognizes that mistakes occur on spacecraft projects. However, sufficient processes are usually in place on projects to catch these mistakes before they become critical to mission success. Unfortunately for MCO, the root cause was not caught by the processes in place in the MCO project.

A summary of the findings, contributing causes and MPL recommendations are listed below.

Root Cause: Failure to use metric units in the coding of a ground software file, "Small Forces," used in trajectory models

Contributing Causes:

1. Undetected mismodeling of spacecraft velocity changes.
2. Navigation Team unfamiliar with spacecraft.
3. Trajectory correction maneuver No. 5 not performed.
4. System engineering process did not adequately address transition from development to operations.
5. Inadequate communications between project elements.
6. Inadequate operations Navigation Team staffing.
7. Inadequate training.
8. V&V process did not adequately address ground software.

Recommendation(s):

1. Verify the consistent use of units throughout the MPL spacecraft design and operations.
2. Conduct software audit for specification compliance on all data transferred between JPL and Lockheed Martin Astronautics.
3. Verify Small Forces models used for MPL.
4. Compare prime MPL navigation projections with projections by alternate navigation methods.
5. Train Navigation Team in spacecraft design and operations.
6. Prepare for possibility of executing TCM No. 5.
7. Establish MPL systems organization to concentrate on TCM No. 5 and EDL operations.
8. Take steps to improve communications.
9. Augment Operations Team staff with experienced people to support EDL.

10. Train entire MPL Team and encourage use of the Incident, Surprise, Anomaly process.
11. Develop and execute systems verification matrix for all requirements.
12. Conduct independent reviews on all mission-critical events.
13. Construct a fault tree analysis for remainder of MPL mission.
14. Assign overall Mission Manager.
15. Perform thermal analysis of thrusters feedline heaters and consider use of pre-conditioning pulses.
16. Reexamine propulsion subsystem operations during EDL.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

Science

Additional Key Phrase(s):

Configuration Management

Flight Operations

Flight Equipment

Mishap Reporting

Software

Spacecraft

Test & Verification

B-19. Public Lessons Learned Entry: 0692

Lesson Info:

- Lesson Number: 0692
- Lesson Date: 1999-02-01
- Submitting Organization: GSFC
- Submitted by: Wil Harkins

Subject:

Coordinate Systems for Attitude Determination and Control

Description of Driving Event:

This Lesson Learned is based on Reliability Guideline Number GD-ED-2211 from NASA Technical Memorandum 4322A, NASA Reliability Preferred Practices for Design and Test.

Benefit:

The primary benefit is increased mission reliability due to a reduction in design errors occurring during spacecraft development caused by inconsistent coordinate frame definitions. A document will be created early in the development of a spacecraft mission defining ACS coordinate frames, which will facilitate data transfer among subsystem engineers, speed documentation and communication during design and analysis reviews, expedite verification of instrument and sensor pointing, and ensure that a record of the coordinate frames used will be available throughout mission planning, design, analysis, and flight.

Implementation Method:

Early in the development stages of a mission program, a document should be created, published, and distributed to all ACS and ACS-related mission engineers. This document will list coordinate frame definitions needed for ACS design and analysis. It should also be periodically updated as mission objectives evolve and hardware changes are made. The following discusses ACS coordinate frame definitions and the format for listing them in the ACS Coordinate Frames Definition Document.

Overview of Coordinate Frame Definitions for ACS Design and Analysis:

ACS coordinate frames contain an origin location and three unit vectors emanating from that origin. “The most convenient set of these vectors is a dextral (i.e., right-handed), orthonormal (i.e., mutually perpendicular and of unit length) triad” [ref. 4, p. 6]. Vector quantities can be expressed as projections onto each of the three triad unit vectors of a coordinate frame. Triads or frames can be related to each other through the use of rotation matrices [ref. 4, pp. 8-10], thus permitting the expression of vectors in any desired frame. With the use of coordinate frames and vectors, the orientation and changes in orientation of spacecraft, celestial bodies, instruments, mechanisms, and other ACS-related hardware and objects can be described.

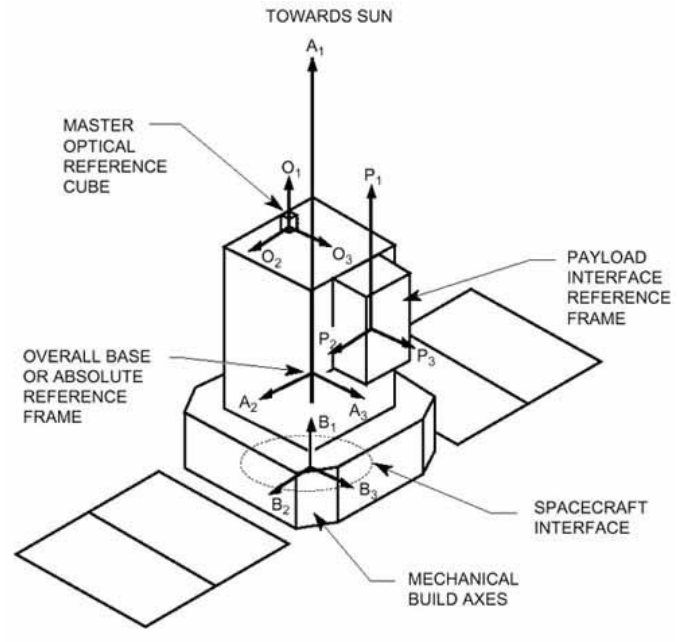
An overall base coordinate frame must be defined relative to which all other coordinate frames are defined. In many cases, this overall base frame will be an inertial frame, which is used to determine overall mission success. For example, if the primary mission of the spacecraft is to point instruments at the Sun, a good choice for the overall base frame might be the heliocentric reference frame [ref. 7, p. 29] since the Sun’s motion can be easily established in this frame.

Typically, within the ACS subsystem, several design issues must be addressed. These design issues can often be arranged into categories, such as overall spacecraft pointing; environmental disturbances; spacecraft mass properties; sensor, actuator, and instrument motion; and flexible body dynamics. A category reference frame should be established to address each design issue. For example, when modeling environmental disturbances in Earth orbit, an Earth-centered inertial frame is usually used as the category reference frame. For defining the spacecraft mass properties; sensor, actuator, and instrument motion; and flexible body dynamics, the category reference is some sort of spacecraft body fixed coordinate frame. If information is to be transferred between these ACS categories, transformations can be established through the overall base coordinate frame discussed previously.

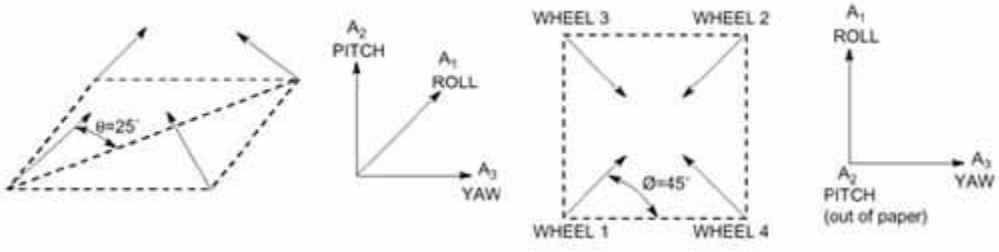
Additional coordinate frames may be needed to define the motion or effect to be modeled within an ACS category. The effect to be analyzed may be defined in terms of an intermediate axis, with this intermediate axis related back to the category reference frame. The coordinate frames needed for defining spacecraft motion within the orbital plane provide a good example of this process. A frame which is fixed to the spacecraft is defined first. This frame is used to define the motion of the spacecraft relative to the orbital plane. Then, a frame fixed to the orbital plane is used to define the motion of the orbital plane relative to an inertial frame. The result will determine the spacecraft motion relative to the inertial frame.

Another example of the use of intermediate axes for addressing ACS design issues is the relationship among sensor and instrument reference frames. One axis of these frames is almost always defined along the boresight of the sensor or instrument. The other two axes should match some other characteristics (e.g., parallel to the edges of a square field of view). The origin is at any convenient point. The relationships of the nominal and “tracking” (i.e., a frame that moves with the boresight to track the sensor motion) boresight frames to the category reference can be achieved in many ways, depending on accuracy and knowledge requirements. Several intermediate frames might be needed to achieve these relationships. Often, both the nominal and tracking boresight frames must be related to a payload interface frame, and all requirements of alignment are specified between this interface frame and the spacecraft optical frame. Typically, the interface frame axes are nominally parallel to the spacecraft optical axes and the optical axes are defined with respect to an optical master reference cube. The nominal position of this cube relative to the spacecraft mechanical build axes (e.g., used for defining hardware locations within the spacecraft) must be defined next. Finally, this mechanical build frame may be used as or related to the category reference. The following figure shows the nominal orientations of these frames used in the SOHO spacecraft [ref. 1, p. 2.8].

This example demonstrates the process of how coordinate frames are used to define the sensor and instrument pointing relative to its category reference frame.



A discussion of the frames needed to model how actuators are used for attitude control is presented as a final example of the use of intermediate frames. Momentum wheels, CMGs, torque rods, and thrusters are commonly used control actuators. Frames are needed to represent the nominal orientation and location, misalignments produced when installing, and movement of the actuators. Also, rotation matrices that relate these frames to the category reference, usually the spacecraft ACS axes, must be determined. As a specific example, consider the frames needed in distributing control torques among a reaction wheel set containing four wheels. The wheels are usually aligned in a pyramid configuration, as shown below. A frame is first defined for each wheel with one axis along the spin axis of each wheel. Then, rotation matrices are created relating each wheel frame to the spacecraft ACS frame (called roll, pitch, and yaw for this case). This example demonstrates how intermediate and category frames are used to relate the orientation and motion of actuators (in this case, reaction wheels) to achieve desired torques.



Document Format:

A suggested format or outline for the coordinate frame definitions document is summarized here. However, this format is only a guide, and the user may need to tailor the format depending on the spacecraft mission. Since the choices of ACS coordinate frames to be defined are dependent on the overall spacecraft pointing objectives and the proposed ACS mission hardware required, these topics should be discussed first. To avoid any ambiguity, coordinate system symbols and nomenclature to be used should be listed next. Specific coordinate frame definitions should

follow—an overall base frame, category reference frames, and frames needed within each category. Finally, a way of relating all the coordinate frame definitions should be included.

ACS Coordinate Frames Definition Outline	
Document Title	
Table of Contents	
Mission Objectives, Requirements, and Criteria for Success	State overall spacecraft pointing objectives and specifications.
Overview of ACS Hardware	State what instruments, control actuators, and other mechanisms are being used for sensing, data collection, and control actuation.
Nomenclature and Symbols	Discuss the nomenclature and symbols to be used for the coordinate frame definitions.
Overall Base Frame Definition	Define a frame to which all other frames are referenced.
Category Frames	Group design issues into appropriate categories, e.g., spacecraft, instrument, and sensor pointing, actuator sizing, environmental disturbances, spacecraft mass properties, etc. Within each category, a category reference frame should be listed along with all other frames needed to address design and analysis issues. Figures showing the physical relationships among these frames would be helpful.
Coordinate Frame Transformations	Relate each frame to the overall base frame.

The first section of the document (after the table of contents) states the overall mission objectives and criteria for a successful operation. The objectives include a list of celestial, Earth based, or other bodies to which the spacecraft and instruments must point. A discussion of the pointing accuracy and knowledge error definitions and specifications for performance needs to be given. Orbit parameters, spacecraft mass properties, and any issues that might affect the mission objectives or success criteria are provided in this section. This section will aid the reader in understanding the rationale behind the choice of coordinate frames.

The second section of the document contains an overview of ACS hardware. Included in this discussion are locations, orientations, and functions of all ACS-related hardware. The locations and orientations are best shown with a figure or a reference to an interface drawing. If the hardware moves or reorients itself (e.g., solar array rotation to track the Sun) relative to the spacecraft, this change is to be documented. The anticipated effects of flexibility should also be considered.

Instrument and attitude sensor functions are given in relation to the overall ACS concept. For example, a magnetometer is used to determine the Earth's magnetic field relative to the spacecraft. The location and orientation of the magnetometer relative to the spacecraft needs to be given, along with a statement of how the magnetometer may be used in conjunction with other ACS hardware and software. The magnetometer output may be used for attitude sensing or

determining when to pulse a torque rod to provide an attitude control moment. These different magnetometer functions may result in different coordinate frame choices.

The third section of the document needs to discuss the nomenclature and symbols to be used for the coordinate frame definitions. The format may vary depending on the spacecraft mission. An example definition taken from reference 6 and shown below demonstrates a possible format for defining reference frames. A descriptive or commonly used name is given first. A one- or two-letter symbol is listed next and also used for labeling the vectors composing the frame axes. Then a description of the frame is provided, and this description is to contain enough detail to unambiguously locate the frame.

Equatorial Inertial Coordinate System E (e.g., E1, E2, E3):

This is the basic inertial coordinate system. All other coordinate systems are defined with respect to E. The origin is at the center of the Earth. The E3 axis is in the equatorial plane, and it is positive toward the vernal equinox. The E2 axis is perpendicular to the equatorial plane, and it is positive toward the Earth's North Pole. (The E1 axis completes the orthogonal triad.) The vernal equinox position is defined as its mean position at 1950.0.

All the frames included in the document are related to the overall base frame. Rotation matrices are commonly used to convert components of vectors from one frame to another, and the development of the mathematics is available in the literature [refs. 4, 6, and 7]. To avoid any ambiguity in the definitions of coordinate frame rotations and their matrices, a discussion of this topic is to be included at the beginning of this section. This discussion should include definitions of Euler angles, quaternions, direction cosine matrices, or other mathematics to be used to relate the frames. Then a table or any convenient format is included at the end of the document to contain information relating each frame back to the overall base frame. Finally, figures illustrating the nominal relationships among all these frames and the possible reorientations of the frames during flight is essential and is included in the document.

Technical Rationale:

Due to the increased complexity of ACS work for spacecraft, a document is needed in the early stages of project development that contains consistent and well-defined coordinate system definitions. Definitions are needed to accurately communicate within and between various design and analysis disciplines affecting ACS performance. These disciplines include spacecraft pointing, environmental disturbances, spacecraft mass properties, sensors, actuators, and instrument motion, structural dynamics, and mechanisms.

Analytical and design mistakes can occur due to communicating erroneous information within and among design and analysis groups. This erroneous communication can be caused by inconsistent or ambiguous coordinate frame definitions. If a document listing coordinate frames to be used for ACS design and analysis is published and adhered to, then many problems can be avoided. For example, an ACS engineer may need to know the mass and inertia of the spacecraft to simulate the dynamics. However, when obtaining this information from structural or design engineers, often the ACS and the structural body frames are not consistent. If a mission standard was established early in the program life, both body frames would be consistent, or at least, the creation of a rotation matrix between frames would be readily obtained.

Documentation of ACS frames would also be clear, consistent, and complete if this guideline is followed. During preliminary and critical design reviews, much time is spent searching for definitions of ACS frames and information relating to those frames. If all the frames are compiled into one document and related to an overall base frame, considerable time and effort will be saved.

Verification of spacecraft, instrument hardware, and other mechanism pointing will be facilitated. Often it is necessary to visually or otherwise make "sanity" checks to ensure component rotations will result in the desired orientation. For example, for Earth-orbiting spacecraft it is necessary as part of the mission systems verification to ensure that spacecraft solar arrays "track" the Sun. To make this verification, the Sun and solar array normal vectors must be written in the same frame and compared. This process involves several coordinate frame rotations, which should be defined in the document generated through this guideline.

An accurate record of these coordinate frames will be available throughout mission planning, development, and flight. If during development of flight hardware and software a technical glitch occurs, it will be necessary to review the ACS design analysis work. Without documented ACS coordinate definitions, analyses may be difficult to validate, causing additional mission costs and delays. Also, ACS engineers will be able to review coordinate frame definitions created with this guideline enabling them to better plan and analyze for future spacecraft missions.

References:

1. Berner, C., "SOHO Solar Terrestrial Science Programme Experiment Interface Document, Part A," PLP/410/EID A, January 7, 1990.
2. Ford, Terry, Spacecraft PDR Update, "EOS Pointing Error Budgets, Prediction, and Verification Concept," EOS-DN-SE&I-043 Rev A, August, 1993.
3. Frederick, Martin E., "Tropical Rainfall Measurement Mission, Attitude Control System Specification," Goddard Space Flight Center, Greenbelt, Maryland, TRMM-712-046, August 13, 1993.
4. Hughes, Peter, C., Spacecraft Attitude Dynamics, John Wiley and Sons, 1986.
5. Kaplan, Marshall, H., Modern Spacecraft Dynamics and Control, John Wiley & Sons, 1976.
6. Kennel, Hans F., "Space Telescope Coordinate Systems, Symbols, and Nomenclature Definitions," Systems Dynamic Laboratory, George C. Marshall Space Flight Center, Alabama, NASA TM X-73343, September, 1976.
7. Wertz, James R., "Attitude Geometry," Spacecraft Attitude Determination and Control, Kluwer Academic Publishers, Netherlands, 1991.

Lesson(s) Learned:

The primary impact of nonpractice is reduced reliability of ACS caused by miscommunication of technical information. The result of mis-communication can vary in severity—from a delay in schedule to resolve any discrepancies to the cost of reworking ACS components to (in the extreme) an un-recoverable mission failure due to ACS design errors.

Recommendation(s):

This guideline provides a procedure that specifies and documents consistent, useful, and well-defined coordinate system (or frame) definitions for spacecraft attitude control design and

analysis. Several example coordinate frames and transformations are presented to show how these definitions are used to address various ACS design issues. Past experience has shown the most efficient convention varies from project to project as a function of mission type, constraints, and performance requirements. This procedure addresses the process and documentation to reliably define the most efficient reference frame convention for a given mission or spacecraft.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

N/A

Mission Directorate(s):

Exploration Systems

Science

Space Operations

Aeronautics Research

Additional Key Phrase(s):

Flight Operations

Launch Vehicle

Payloads

Spacecraft

Approval Info:

Approval Date: 2000-03-13

Approval Name: Eric Raynor

Approval Organization: QS

Approval Phone Number: 202-358-4738

B-20. Public Lessons Learned Entry: 0711

Lesson Info:

- Lesson Number: 0711
- Lesson Date: 1999-02-01
- Submitting Organization: GSFC
- Submitted by: Wil Harkins

Subject:

Magnetic Field Restraints for Spacecraft Systems and Subsystems

Description of Driving Event:

This Lesson Learned is based on Reliability Practice No. PD-ED-1222; from NASA Technical Memorandum 4322A, NASA Reliability Preferred Practices for Design and Test.

Benefit:

Limits magnetic field interference at flight sensor positions and minimizes magnetic dipole moments that can increase magnetic torquing effects that place additional loads on ACSs.

Implementation Method:

A magnetic test procedure has been established which includes separate determinations of the permanent, induced, and stray field magnetization of parts and sub-assemblies. These three conditions represent the prominent sources of spacecraft magnetic field restraint problems. Applied field vectors are utilized to determine the induced magnetic field properties which the spacecraft will experience in orbit. The stray field measurements are designed to differentiate between the power-on vs power-off conditions of operation as well as the shifts in the stray-field levels during operation of the equipment. In the case of the permanent magnetization measurements, the following conditions or states are normally measured:

1. **Initial Perm.** "As received" magnetic state of the item, which indicates:
   a. One possible level that may exist for a newly manufactured item of the same design.
   b. A relative field magnitude used to determine deperm treatment effectiveness.
   c. The stability of perm by initiating a record of its magnetic history.
2. **Post Exposure.** Magnetic state of the item after exposure to a 15 or 25 gauss DC magnetic field, which represents the most probable maximum field to which the item is expected to be exposed during environmental testing.

A. Post Deperm. Magnetic state of the item after being demagnetized in a 50 gauss field (normally 60 Hz AC field). Reference 1 provides further data related to methods of demagnetization and compares the results obtained.

A substantial amount of test data has been accumulated relating to the magnitudes of magnetic field for various components normally used in spacecraft systems by indicating the magnetic field disturbance in gamma (10-5 oersted) at a distance of 12 in. from the center of the item. These magnitudes have been measured directly or extrapolated, (by inverse cube) from supplementary distance data. In many cases two or more identical items were measured to insure more representative data; however, in those cases only the maximum value has been listed. In the

case of particular components which are required to be non-magnetic, i.e., resistors and connectors, the data is presented for the distance of 2 in. This data is intended to represent the various magnetic field levels to be expected from the items rather than representing an acceptable or nonacceptance parts list.

Magnetic test data has been accumulated from tests of various types of batteries used in flight programs such as IMP, UA-2, OAO, OGO, MMS, and DE. These data show that cells with the nonmagnetic silver cadmium electrodes should be used for spacecraft containing magnetic field experiments. Nickel Cadmium cells should be particularly avoided since these cells have a substantial permanent magnetic field characteristic due to the presence of the nickel material. In the case of other spacecraft where the nonmagnetic requirements are not quite as stringent, it might be more desirable to use the nickel cadmium cells because of their preferred electrical characteristics. While the use of silver cadmium cells will minimize the permanent magnetic field disturbance, their use will not reduce the stray field disturbance which depends on the current flow in the individual cells as well as the combined terminal connection arrangement. Reduction and cancellation of the stray field can be best achieved in those cases where an even number of cells have been combined to form the complete battery pack. Cancellation of the stray field, would be accomplished by combining the cells back-to-back in pairs so that the stray field of one cell effectively opposes that of the other. When an odd number of cells is combined, the stray field of the one unmatched cell can be canceled by adding a supplementary loop of wire which generates a stray field in opposition to that of the single uncompensated cell.

Similar magnetic test data has been accumulated for a variety of flight capacitors, connectors, various materials and products such as metals and alloys, electric motors, relays, wiring, etc. These tests were performed a number of years ago and the test samples may not represent some of the materials and components used in more recent years. The magnetic test technique and the approach used in selecting materials with suitable magnetic characteristics can provide a guide to the testing and selection of newer materials and components.

References 1–3 provide more details on the testing and include many tables of test data.

Technical Rationale:

The problem associated with magnetic field restraints for components and spacecraft vary according to the spacecraft program requirements. Spacecraft that include magnetic field experiments must control and limit the magnetic field disturbance of the integrated spacecraft so that no undue magnetic field interference will occur at the flight sensor positions. In the case of spacecraft that employ magnetic or gravity gradient attitude control systems, the magnetic restraint problems are normally not as stringent. However, all spacecraft designers should avoid the use of components and sub-assemblies with significant magnetic moments since these will increase magnetic torquing effects and place additional loads on the ACS.

This practice is primarily intended for use by spacecraft programs subject to magnetic field restraints, i.e., spacecraft containing magnetic field experiments or magnetic attitude control systems. Accordingly, it can be used as a guide in the magnetic testing, assessment, and selection of parts and materials to be used by such programs.

References:

1. “Magnetic Field Restraints For Spacecraft Systems And Subsystems,” February 1967, GSFC Document No. X-325-67-70.
2. Supplement 1 (1971) to “Magnetic Field Restraints For Pacemaker Systems and Subsystems,” December 1971, GSFC Document No. X-325-71-488.
3. “Spacecraft Magnetic Test Facility (Attitude Control Test Facility),” April 1984, GSFC Document No. X-754-83-9.
4. Reliability Preferred Practice No. PD-ED-1207, “Magnetic Design Control For Science Instruments.”

Unit Conversions:
1 gauss = .1 millitesla (mT)
1 oersted = 79.57747 ampere/meter (A/m)
1 inch = 2.54 centimeter (cm)

Lesson(s) Learned:

If this practice is not followed, appropriate magnetic field restraints on components and systems may not be employed and the resulting magnetic interference could significantly interfere with the proper functioning of magnetic field experiments. Also, any high level magnetic dipole moments would increase magnetic torquing effects and place additional loads on ACSs.

Recommendation(s):

Control magnetic field disturbance of spacecraft systems by avoiding the use of components and sub-assemblies with significant magnetic dipole moments.

Evidence of Recurrence Control Effectiveness:

This practice has been used on OGO, EPE-D, IMP, Pioneer, AE-B, ATS, DME, OAO, ISTP, GRO, EUVE, Ulysses.

Documents Related to Lesson:

N/A

Mission Directorate(s):
Exploration Systems, Science, Space Operations, Aeronautics Research

Additional Key Phrase(s):
Flight Equipment, Hardware, Launch Vehicle, Parts Materials & Processes, Payloads, Spacecraft

B-21. Public Lessons Learned Entry: 0726

Lesson Info:

- Lesson Number: 0726
- Lesson Date: 1999-02-01
- Submitting Organization: GSFC
- Submitted by: Wilson Harkins

Subject:

End-To-End Compatibility and Mission Simulation Testing

Description of Driving Event:

This Lesson Learned is based on Reliability Practice Number PT-TE-1437 from NASA Technical Memorandum 4322A, NASA Reliability Preferred Practices for Design and Test.

Benefits:

This testing significantly enhances flight reliability by ensuring that all portions of the flight operational system work together as expected. This includes the proper flow of data to the end users.

Implementation Method:

The GSFC Mission Operations and Data Systems Directorate (MO&DSD) develops, maintains, and operates a worldwide Ground Data System (GDS) to support a wide range of flight missions. Various organizational units within the MO&DSD such as branches, sections, and mission readiness test teams collaborate with the Flight Project and the Flight Assurance Directorate in planning and performing a wide range of mission readiness testing. The purpose of this readiness testing is to verify the performance and demonstrate the readiness of the integrated GDS to support specific flight missions. This practice is implemented by the MO&DSD in the following three basic phases.

Phase A: Acceptance and Interface Testing of Individual GDS Elements

Acceptance and interface testing is performed on each GDS element for each flight mission. This testing is particularly applicable to hardware and software elements in the GDS that have been updated, modified, or added to meet specific mission requirements.

The acceptance and interface testing is followed by a formal Project Integration and Test Program. The Project Integration and Test Program verifies that the GDS can meet all of the project mission support requirements and documents the system's operational readiness. After all requirements have been verified, all discrepancies have been resolved, and all corrective actions have been completed, the verification process through Integration and Test is complete. The GDS is now ready to participate in Phase B, Compatibility Testing.

Phase B: Compatibility Testing

Compatibility testing is conducted on all portions of the operational system, including the payload, the operational software, and the ground systems. The ground systems include the Space and Ground Networks, the Mission Operations Control Center (MOCC), and the data processing facilities. When the mission scenario calls for electrical operation of the payload

aboard or in conjunction with the STS, compatibility of the operational system is demonstrated with the use of the appropriate elements of the STS, such as the Orbiter Payload Data Handling System and the Mission Control Center. After completion of compatibility testing, the GDS is ready to participate in Phase C, Mission Readiness and Mission Simulations Testing.

Phase C: Mission Readiness And Mission Simulation Testing

Mission Readiness Testing is conducted to verify that system design specifications are being routinely met, ascertain the level of operational proficiency being maintained throughout the networks, and evaluate the network's abilities to meet or exceed design specifications in response to project requirements. An evaluation phase follows in which all Discrepancy Reports (DRs) are reviewed by a DR Review Board.

Mission Simulation Testing includes data flow tests performed on the total system in a realistic mission timeline. When practical, external stimulus of the spacecraft instruments and attitude control sensors are used.

Mission Readiness and Mission Simulation Testing is carried out in accordance with formal test plans prepared and approved by the MO&DSD with concurrence by the flight projects. These test plans define test coordination, system requirements, test procedures, problem resolution procedures, and reporting requirements. In order to ensure an integrated testing effort, testing and planning is coordinated through a Mission Readiness Test Team comprised of project and MO&DSD development, test, and operations representatives.

Test Facilities and Systems Used for Compatibility and Simulations Testing

This section on test facilities and systems used for compatibility and simulation testing provides a description of the major elements of the GDS and how they are used in these test programs.

The Simulations Operations Center (SOC) located at GSFC provides support and test tools that can emulate the spacecraft, the MOCC, the Network Control Center, and the Ground and Space Networks. System evaluations and validation test and simulation programs are also conducted to characterize new or modified Space and Ground Network (GN) capabilities, to verify that system design specifications are being met routinely, to ascertain the level of operational proficiency being maintained throughout the networks, and to evaluate network abilities to meet or exceed design specifications in response to user requirements. The SOC provides various resources used to simulate and test ground data system elements. These resources include the Project Platform Training Simulator, the SOC Mission Control Simulator, the RF Simulations Operations Center, the Portable Simulations System, and various utility programs, such as a Super Programmable Data Formatter and the data blocker/deblocker. The SOC has a standard NASA Communications (NASCOM) interface, which permits it to communicate with all ground data system elements during Simulation and End-to-End Testing.

The Platform Training Simulator provides support for training the Flight Operations Team (FOT) in normal and contingency spacecraft operations. The FOT can refine and practice operations and contingency procedures without using valuable spacecraft time. The simulator is also used to support the Integration and Test data flows and Network Simulation tests.

The SOC Mission Control Simulator emulates JSC's payload support functions for simulations with the MOCC.

The RF SOC is a simulations facility used for Space Network (SN) simulations and data flows. It has the capability to communicate with the Tracking and Data Relay Satellite E through a small satellite earth terminal located at the GSFC.

The Data Evaluation Lab (DEL) provides recording systems, engineering support, and special data services. It can generate, quality check, and provide distribution for pre-mission simulation tapes and analog tapes. Additionally, the DEL can play back generated tapes in the form of data flow to the Mission Operations Center (MOC) and other elements in support of engineering, pre-mission, and operational readiness tests.

The SUPER Programmable Data Formatter (PDF) is a portable, stand-alone system used in the SOC or at remote sites for ground system data flow tests, interface verification tests, and end-to-end rehearsals. The SUPER PDF can generate simulated real-time and playback telemetry. It is packaged in a portable unit for supporting tests from the GN, spacecraft integration areas, or launch sites.

Mobile Compatibility Test Vans (CTVs), normally stationed at the GSFC, travel to the spacecraft factory or launch site. They are used for verifying the spacecraft's RF compatibility with the network by performing initial checkout of the spacecraft RF interface with the tracking and data networks. The CTVs also provide the MOCC with a direct link to the spacecraft at the manufacturing plant. The CTV can send spacecraft telemetry data via the GN and NASCOM to all support elements and can receive commands from the MOC via the SN and the NASCOM. They can also be used as a data source for performing network verification tests.

Monitoring and Witnessing of GDS Testing

The GSFC Office of Flight Assurance assigns an Assurance Management Representative (AMR), a Systems Assurance Manager, and others as needed to perform assurance functions on flight projects. These functions include identifying tests to be monitored or witnessed, determining the level of coverage based on the test objectives and criticality, and arranging for the coverage by assurance representatives or their contractors. The assurance functions also include observing and reporting on the success of the test in meeting its objectives. The results are documented and identify any events or anomalies for use by engineering and management. The AMR test report contains the objectives of the test, anomaly reports, corrective actions expected, and the AMR's appraisal of whether test objectives were met.

Technical Rationale:

The detailed performance of the GDS in meeting the specific technical requirements of spaceflight missions is thoroughly evaluated and validated in order to ensure mission readiness and compatibility with mission requirements. This readiness includes the training of control center operational personnel by simulating and practicing both nominal and contingency flight operations.

References

1. GSFC Document, “Directorate Test Support,” Subject – Code 500 Directorate Test Support.
2. GSFC Document, “Flight Assurance Procedure,” No. P-303-1025, Subject-Monitoring and Witnessing GDS Testing.
3. GSFC, SPAR-3, Standard Payload Assurance Requirements (SPAR) for GSFC Orbital Project, Paragraph 3.7, March 1990.

Lesson(s) Learned:

Nonpractice of End-to-End Compatibility and Mission Simulation Testing could result in marginal performance or failure of the mission due to incompatibilities in the Ground Data System. Control center operational errors due to inadequate training could significantly impact the health and safety of the spacecraft.

Recommendation(s):

End-to-End Compatibility and Mission Simulation testing are conducted on all portions of the GDS. These tests are performed to fully demonstrate the operational compatibility and the ability of the entire system to perform as expected during the flight mission.

Evidence of Recurrence Control Effectiveness:

This practice has been used on all flight programs managed by GSFC. They are required to use this practice.

Documents Related to Lesson:

N/A

Mission Directorate(s):

Exploration Systems

Science

Space Operations

Aeronautics Research

Additional Key Phrase(s):

Communication Systems

Flight Equipment

Ground Equipment

Hardware

Launch Process

Launch Vehicle

Payloads

Risk Management/Assessment

Spacecraft

Test Article

Test Facility

Test & Verification

Approval Info:

Approval Date: 2000-03-30

Approval Name: Eric Raynor

Approval Organization: QS

Approval Phone Number: 202-358-4738

B-22. Public Lessons Learned Entry: 1370

Lesson Info:

- Lesson Number: 1370
- Lesson Date: 2002-06-11
- Submitting Organization: JSC
- Submitted by: John L. Goodman

Subject:

Lessons Learned From Flights of "Off the Shelf" Aviation Navigation Units on the Space Shuttle, GPS

Abstract:

Over the last 9 years, the Shuttle Program has flown GPS receivers and Space Integrated GPS/Inertial Navigation System (SIGI) units. The NASA Johnson Space Center paper, "Lessons Learned From Flights of 'Off the Shelf' Aviation Navigation Units on the Space Shuttle" contains numerous recommendations that constitute the body of this lesson.

Description of Driving Event:

The Space Shuttle program began flying atmospheric flight navigation units in 1993, in support of Shuttle avionics upgrades. In the early 1990s, it was anticipated that proven in-production navigation units would greatly reduce integration, certification and maintenance costs. However, technical issues arising from ground and flight tests resulted in a slip in the Shuttle GPS certification date.

A number of recommendations were developed concerning the adaptation of atmospheric flight navigation units for use in low-Earth orbit. They are applicable to any use of a navigation unit in an application significantly different from the one for which it was originally designed. Flight experience has shown that atmospheric flight navigation units are not adequate to support anticipated space applications of GPS, such as autonomous operation, rendezvous, formation flying and replacement of ground tracking systems.

Space Shuttle Tactical Area Navigation (TACAN) Replacement with GPS

In 1990, the Shuttle Program began to investigate the use of GPS, based on the anticipated phase-out of TACAN starting in the year 2000. The Shuttle Program desired a receiver that was in mass production and had an existing logistics base. Anti-jam and anti-spoofing capabilities were also desired. A trade study conducted in 1993 chose the five-channel Miniaturized Airborne GPS Receiver (MAGR), which entered production in 1994. The MAGR/Shuttle, or MAGR/S, was procured as a TACAN replacement and for use as a source of state vectors while on-orbit. There were no requirements for the MAGR/S to be used for applications involving high-accuracy orbit determination, such as ground radar and TDRSS tracking replacement or spacecraft rendezvous. The MAGR/S will be certified to serve as a TACAN replacement in both keyed and unkeyed configurations. No requirements were levied on the vendor to change the MAGR/S Kalman filter, which was designed for use on a variety of aviation platforms without modification. An orbital state vector propagation algorithm was added to support satellite acquisition after a GPS outage.

A pre-production MAGR, called the 3M, was flown seven times on the Shuttle Endeavor from December 1993 to May 1996. The first flight of a production MAGR missionized for the Shuttle application (MAGR/S) occurred in September of 1996. By the fall of 1997, five test flights of the MAGR/S on the Space Shuttle had occurred. At that time, the Shuttle Program decided to replace the three TACAN units on Atlantis with three MAGR/S units. The first "no TACAN, all GPS" flight was scheduled for January 1999 (STS-92).

By June of 1998, the first flight of Atlantis with three-string GPS had changed to STS-96 (May 1999), due to changes in the ISS assembly schedule. While on-orbit during STS-91 (Discovery, June 1998), the final Shuttle-Mir mission, a MAGR/S firmware problem and several flaws in the Space Shuttle computer software that communicate with the MAGR/S were discovered.

Certification of the MAGR/S was postponed. MAGR/S firmware and Shuttle software issues were resolved, and additional MAGR/S firmware versions, ground and flight-testing were planned. Certification of the MAGR/S for operational use occurred in 2002. However, it is not known when the Shuttle Program will decide to replace the TACAN units with the MAGR/S receivers. With the start of TACAN phase-out delayed until 2010, it is expected that the Shuttle Orbiters will fly with three TACAN units and one MAGR/S receiver for some time.

Three Shuttle flights (STS-81, -84 and -86) carried embedded GPS/INS (EGI) units from two vendors to collect data for the X-33 program.

In 1996, NASA began a project to eventually replace the MAGR/S receivers and the HAINS IMUs with a space-missionized EGI, known as a SIGI. SIGI was envisioned as a "common NASA navigator" that could be used on a variety of crewed and uncrewed vehicles. The Shuttle SIGI flew on seven missions between September 1997 and December 1999 for data collection. Since the HAINS IMUs were projected to be operational through 2010, replacement of the HAINS IMUs and MAGR/S units by SIGIs was deferred.

Lesson(s) Learned:

The Shuttle Program selected off-the-shelf GPS and EGI units that met the requirements of the original customers. It was assumed that off-the-shelf units with proven design and performance would reduce acquisition costs and require minimal adaptation and minimal testing. However, the time, budget, and resources needed to test and resolve firmware issues exceeded initial projections.

Recommendation(s):

1. A realistic schedule and budget is needed. Particular attention should be paid to how realistic the schedule is considering the complexity and technical risk involved. A recent study of NASA projects that used a FBC approach indicated that mission failures resulted from highly complex projects on short development timelines.
2. Fixed-price contracts should be avoided if development work is required. Such contracts can result in inflated vendor estimates for initial cost and can remove the incentive to aggressively resolve technical issues. Resolution of these issues may not be covered in the budget defined at project start.

   Technical issues must be addressed early in a project, even in the presence of cost and schedule concerns. These issues can easily become showstoppers later in the integration. Not

addressing issues until late in a project will drive up cost and shift schedules to the right. Problems arising from cost and schedule slips and failure to address issues can create adversarial relationships between project participants and the vendor.

Fixed price contracts are appropriate when the planned use of the unit is the same as the original application for which the unit was designed. In this case, little or no development work is required. Modifying an aviation navigation unit for use on an unmanned or manned spacecraft should be budgeted and scheduled as a development project.

3. Resources and schedule must be allocated to analyze test data. When planning a navigation unit missionization and integration, adequate time and personnel must be set aside to analyze flight and ground test data. If data is not thoroughly analyzed in a timely manner, firmware issues will go unnoticed. Lack of resources can even lead to failure to analyze test data. Performance issues arising late in the development and certification cycle can negatively impact cost and schedule.

4. Maintain an integrated team approach. The "success-oriented" nature of project budgets and schedules sometimes result in limited communication at the technical level. Multiple layers of contractors cut down on communication and should be avoided. The vendor should be involved in all design reviews.

   Early MAGR/S project reviews focused on hardware modifications, with little attention paid to firmware. Most technical personnel were firewalled from the firmware missionization process and the vendor. No formal, program-wide reviews of the GPS receiver firmware modifications were made. The GPS vendor and Shuttle navigation (operational and engineering, contractor and civil servant) personnel had minimal involvement in the missionization decisions made by the integrator.

   The GPS vendor was more fully integrated into the GPS project to enhance communication due to anomalies that surfaced during STS-91. Weekly teleconferences were established that included the vendor and all NASA and contractor organizations. Face to face meetings of all project participants were held at the Johnson Space Center three to four times a year. Special teams that crossed civil servant and contractor boundaries were formed to address specific technical problems.

   The GPS receiver is a critical part of an EGI. Unfortunately, the user and integrator often have little or no opportunity to interact with the GPS manufacturer on an EGI contract. Contracts concerning EGI units should be written so that the GPS vendor will be involved and able to give advice and information to the EGI manufacturer, the integrator, and the user.

5. Produce, test, and fly interim firmware versions. Firmware issues tend to be discovered sequentially. Units containing complex firmware may not manifest anomalies in the initial round of ground and flight tests. This can lead to a false sense of security about the maturity of a firmware version. Enough rigorous ground and flight testing must be planned to thoroughly exercise the firmware. Schedule and budget should include interim firmware versions to allow issues to be discovered and resolved before a production firmware load is scheduled for certification.

6. Keep accurate records. Detailed and accurate records of meetings, issues, issue disposition, and design rationale should be maintained. This enables project participants to be better

informed on issues facing the project and provides a record for the future. An official issue list should be maintained, along with a list of questions for the vendor and vendor responses.

7. A close relationship between the vendor and customer is needed. Both the MAGR/S and SIGI projects demonstrated the need for a close working relationship between the integrator, users, and vendor. The navigation vendor needs to be involved in early decisions on architecture and integration. Frequent and open communication between technical personnel should be encouraged. This lesson is best summed up as "communicate early, communicate often." The "throw a unit and an ICD over the fence" approach can lead to cost and schedule problems.

   Due to communication constraints imposed by "success-oriented" budgets and schedules, vendors are frequently not involved in the design of software that is to interface with a GPS or EGI unit. In hindsight, some aspects of the Shuttle GPS integration might have been done differently had the vendor been involved. The Shuttle software that interfaced with the MAGR was designed with an inadequate understanding of the firmware behind the interface definition. This lack of receiver insight was one of the causes of the problems encountered on STS-91. Shuttle software that interfaced with the GPS receiver had to be bullet-proofed against known and postulated receiver anomalies.

   Regular face-to-face contact between the vendor and Shuttle engineers built positive, personal relationships and established a "team" rather than an "adversarial" environment. Communication between other project participants also improved. Vendor and Shuttle Program engineers became familiar with each other's work cultures, which enabled them to work better together and provide appropriate support to each other. The vendor also provided much-needed education to Shuttle engineers concerning the challenges of GPS receiver design and operation.

   Use of complex, off-the-shelf aviation navigation units in unmanned and manned space applications requires vendor involvement over and above that provided in terrestrial aviation projects.

8. Educate the vendor about your application. The GPS vendor observed Space Shuttle ascents and entries from Mission Control. Vendor GPS engineers also flew landings in a Space Shuttle simulator and were present in the cockpit of the Shuttle Avionics Integration Laboratory when MAGR/S testing was performed. They also participated in lab tests of the MAGR/S at Shuttle Program facilities. These activities permitted the vendor to ascertain how the Space Shuttle application differed from aviation users of GPS receivers. These experiences were helpful in understanding customer concerns and identifying improvements to be made to the receiver. This enabled the vendor to propose solutions to technical issues that were agreeable to the various parties within the project.

   The vendor became familiar with the strengths and weaknesses of Shuttle Program GPS simulation facilities. This enabled them to provide input to Shuttle integration engineers concerning how best to perform receiver testing and verify MAGR/S functionality.

9. Talk to those who have used the product before. Outside consultants who have no stake in the choice of a particular unit should be used. Such consultants have hands-on experience with box integrations and can be an important information source concerning their design,

integration, and use. Consultants who have participated in previous integrations will have knowledge of problems other users have encountered. Consultants and other users can also provide valuable insight into the rationale and requirements that governed the original unit design. This information is invaluable to the integrator for identifying technical, cost, and schedule risks associated with a particular navigation unit integration.

10. "Plug and play" versus development. The fact that a unit is in mass production and is a proven product does not mean its integration into a different vehicle will be a simple, problem-free "plug and play" project. A difference in application (e.g., aviation versus space flight) will result in the manifestation of firmware issues that may not have appeared in the original application. Unique data interfaces used by crewed and some uncrewed spacecraft avionics may require modification of the unit. Power supply changes and radiation hardening may also have to be performed.

11. Test as much as you can. A lack of comprehensive, end-to-end testing has resulted in a number of spacecraft failures. Deep integration of systems makes them more vulnerable to software issues. As navigation systems become more complex and more deeply integrated, software quality and verification become more important. Firmware development schedules driven by "time to market" pressures and a desire to lower overhead costs (e.g., a small group of programmers, short development and test cycles) result in a higher probability of code with bugs.

    Navigation projects for the Shuttle, ISS and CRV programs reaffirmed the need for rigorous and thorough flight and ground testing. Lab testing using signal generators will not exercise all possible logic paths within a GPS receiver or EGI. Signal generators will not completely duplicate the radio-frequency environment encountered during flight. Receiver anomalies will appear in flight tests that may not manifest during lab testing. Conversely, some anomalies found during lab testing did not occur in flight.

    Many firmware issues could have been found earlier in the Shuttle GPS project had a thorough ground test program been conducted. A limited number of lab and flight tests to ensure that the box "meets spec" will not exercise enough of the firmware to find issues. This is particularly important for safety of flight applications involving humans. Vendors tend to perform the minimum amount of lab testing needed to ensure that the unit meets contract specifications. Vendors may not consider flight-testing to be valid if they do not trust the source of "truth" vectors.

    Testing should also involve any hardware and software that interfaces with the unit. Thorough offline testing of the unit and proposed algorithms that will interface with it should be performed before committing to specific integration architecture. Once the integration has been performed, thorough testing of navigation unit interaction with the rest of the avionics system is needed.

    Some firmware issues resulted from the use of aviation GPS receiver algorithms at orbital altitude. However, many of the firmware issues that surfaced during the MAGR/S and SIGI flight tests were due to basic computer science issues. Firmware issues that do not manifest in aviation applications due to a flight time of minutes or hours can manifest during a much longer space flight. Shuttle program ground and flight-testing of GPS receivers and EGIs has

uncovered many firmware issues that may aid the maintenance efforts of other users of similar units.

End-to-end testing, over the complete flight profile, is required. For space applications, lab tests lasting days or weeks should be conducted. Use good engineering judgment when dispositioning issues, backed up with ground test and flight data.

12. Instrumentation port data is needed during flight and ground tests. Instrumentation port data provides invaluable insight into firmware behavior during periods of questionable performance. Vendor input should be solicited concerning what data to collect and how it should be interpreted. Instrumentation port data simplifies and speeds up the identification of firmware problems. Software on data collection platforms (e.g., laptop computers) must be fully tested, documented and certified. Clear and accurate procedures for laptop operation and troubleshooting are needed. Otherwise, it may be difficult to distinguish GPS receiver problems from problems with the data collection computer.
13. IV&V is invaluable. The NASA IV&V contractor played a significant role in the MAGR/S project. Initial IV&V involvement focused on the integration architecture, ground test, and flight test results. After MAGR/S certification was postponed in 1998 and MAGR/S firmware was made available to the Shuttle Program, IV&V performed an audit of the firmware starting in 1999. The audit was invaluable in the certification process, but should have been conducted much earlier in the MAGR/S project. To date, over 250 issues (of varying degrees of seriousness) have been identified and dispositioned through the IV&V analysis of the MAGR/S requirements and firmware.

    The trend to use NDI avionics containing proprietary software may prevent independent validation and verification of firmware. This is an issue for applications that involve human safety and unmanned applications requiring a high degree of autonomy. The ground and flight test environments will not be able to produce conditions needed to reveal all firmware issues or verify all firmware modifications and fixes. Code audits are needed, both by the vendor and an IV&V organization. Guidelines should be created concerning audit scope and the definition of credible failure scenarios. Lack of an IV&V level firmware audit will result in lingering suspicion about a unit.
14. Conduct enough test flights before making critical decisions. Initial flights of the 3M receiver (pre-production MAGR) were successful. Later flights of the MAGR/S, along with ground testing and firmware audits, uncovered many issues that had to be resolved before the MAGR/S could be certified for TACAN replacement. It is important not to be lulled into thinking problems are not out there based on a small number of initial, successful test flights. Numerous firmware issues were discovered during the STS-91 flight in June 1998, resulting in the postponement of MAGR/S certification for operational use. However, the three TACAN units had already been removed from the orbiter Atlantis and three MAGR/S had been installed. The Shuttle Program had to remove three string MAGR/S and reinstall three string TACAN in Atlantis.
15. Design insight is necessary. Inadequate and outdated documentation and a lack of understanding of output parameters make operation, performance analysis and problem resolution difficult. Lack of design insight also complicates risk assessment of firmware

issues. A lack of formal procedures for operating the unit in the test (flight and ground) environment results in user errors, which cause schedule slips.

Integrators and users have little access to vendor engineers and design documentation. Vendor engineers are often not prepared to answer complex, “spur of the moment” questions at design reviews. Design insight questions require time to research. Trying to obtain design information in the presence of firewalls wastes time and money. Knowledge of product design and operation should not be isolated to a select few. Open and accurate communication is needed. An official questions list should be maintained to record open questions, question status and closure.

A lack of configuration-controlled documents can lead to incorrect knowledge about box design, operation and performance. Inadequate understanding of navigation unit design and operation can also lead to misinterpretation of test results. This makes problem resolution more expensive. A lack of accurate, detailed product documentation forces integrators to spend significant amounts of lab time trying to get the unit to work properly. Frequent consultations with the vendor drives up project costs.

During a mission, operators of both unmanned and manned spacecraft live by their data. Wrong information can lead to making the wrong decisions when faced with a spacecraft anomaly. This can lead to loss of data, some vehicle capabilities or even the spacecraft itself, as in the 1997 Lewis satellite incident.

For a flight critical application (i.e., the box is required to safely conclude the mission), a box will undergo more modification than in other applications. The user will also require more detailed knowledge of navigation unit design and operation than users of non-flight critical units. The Shuttle program considers a box to be failed more quickly than an aviation user. Engineering and Mission Control personnel must have a thorough understanding of receiver operation and data. For manned space flight, lack of design insight is a safety issue. Due to the anomalies that occurred on STS-91, MAGR/S firmware requirements, the integration guide and source code (originally developed at government expense) were made available to the Shuttle program.

Answers to navigation unit insight questions were limited to “how” and often did not include “why.” The “why” often touched on assumptions made in designing a receiver for terrestrial aviation applications.

Assumptions made during the original design can manifest as firmware and receiver performance issues if the assumptions are not valid in the new application of a unit.

During the relative GPS experiments conducted on STS-69 and STS-80, lack of insight into the 3M, TurboStar, Tensor and Quadrex receivers made integration, data processing and data analysis more difficult. In addition, lack of insight into algorithms (particularly those associated with clock steering) made development of the laptop based relative GPS navigation filter more challenging.

Integration engineers must have access to testing facilities and data so they can become familiar with box performance. As more insight is gained about a unit, the ICD and software requirements for the unit and other units that it interfaces with should be examined for errors and inconsistencies.

16. Pay attention to technical risk. Project management may focus mainly on risk to cost and schedule, with little attention paid to technical risk. GPS project management kept Shuttle Program management well aware of the nature of a "success-oriented" approach and that cost and schedule could be impacted. Analysis at the start of a project should be conducted to determine risk to cost and schedule based on the technology level, the maturity of the technology and the difference between the planned application and the application for which the box was designed originally. Software complexity should also be examined. Failure to account for technical risk can lead to cost and schedule problems.

    An additional risk in using off-the-shelf units concerns vendor availability. Can a user continue to use and maintain a product if the vendor goes out of business or stops producing and supporting the product?

17. Coding practices used in the past still haunt users. Many navigation units use firmware descended from systems built over 20 years ago. In the past (and even in the present), good software coding standards were not always used and were often insufficient. New products tend to be developed quickly, with little effort expended on rigorous requirements definition and documentation. Many navigation system vendors maintain a common library of software modules. Different products share many modules. Cost and schedule considerations may lead integrators, users and vendors to ignore firmware issues, rather than fix them. A firmware problem that is no impact to the user that discovered it may be a "show stopper" in a different application. This leads to error propagation through a product line.

    A good example from another program: The Ariane 5 flight 501 launch failure in June of 1996 resulted from the use of code from another launch vehicle. Ariane 4 navigation software was used in the Ariane 5 navigation software. No analysis was performed to determine if the ported code was appropriate for the Ariane 5 application. Several lines of navigation code capable of producing math errors had no protection against such errors. The rationale for not providing error protection was not documented. Furthermore, the launch vehicle computer was not designed to meet any requirements concerning handling and recovery from software errors. Only random hardware errors were taken into consideration.

18. Identify and resolve legal issues concerning proprietary documentation. If a COTS device contains proprietary firmware, legal arrangements must be made to permit inspection of proprietary documentation. Lack of access to proprietary documents can result in undetected issues. One such example, on a civilian spacecraft, was the telemetry bandwidth problem on the European Space Agency Cassini/Huygens Titan probe. This issue was not discovered until the probe was en route to Saturn. Factors that contributed to the late discovery of the problem were lack of access to proprietary documentation, no "end to end" system testing and a lack of comprehensive project requirements.

19. Maintain configuration control over test equipment and procedures. Perceived anomalous navigation unit performance in the lab is more likely to be caused by improper test equipment configuration and improper procedures, rather than firmware or hardware problems in the box or GPS satellite problems. A lack of accurate, documented test procedures can make it difficult to duplicate questionable performance in later tests. This lengthens the amount of time it takes to determine the cause of suspect behavior. When

trying to diagnose questionable performance, an accurate record of what procedures were performed and the test equipment hardware and software configuration is invaluable.

20. Provide the vendor with as much data as possible. Vendors often complain that users provide minimal data when a problem with a navigation unit occurs. GPS receivers are complex computers whose performance depends on a variety of factors. A plot illustrating questionable position and velocity performance is not enough to permit a vendor to diagnose the true cause of an alleged anomaly. The vendor should be provided with as much digital data as possible, particularly channel and tracking parameters. Information on antenna location, hardware configuration and the procedures that were executed is also helpful. Navigation unit vendors are busy and receive large numbers of "calls for help" from the user community. Users who suspect a unit is malfunctioning should make a thorough investigation to determine if the alleged performance is a user error before involving the vendor.

21. COTS box outputs may not be designed with redundancy management in mind. Most aircraft and missiles use only one GPS receiver, stand-alone INS or EGI. Some vehicles (e.g., Space Shuttle, ISS, X-33, X-38) were designed to use multiple navigation units for redundancy. Redundancy management schemes perform checks on box outputs, such as dynamic parameters (e.g., position, velocity, attitude, rotational rate and accumulated sensed velocity) and health status parameters (e.g., BIT/BITE). Most BIT/BITE indicators and self-tests were designed to help ground personnel determine if a suspect unit should be returned to the depot for maintenance.

    Use of BIT/BITE indicators in RM algorithms requires that the integrator understand what the health status indicators mean and how indications of a problem can affect navigation unit performance. Care must be taken when determining which parameters to monitor for assessing unit health. A "title" of what the indicator is in an interface control document does not tell the integrator the potential impact the annunciated condition has on box performance. This makes it difficult for the integrator to determine which BIT/BITE indications should be used in the RM algorithm. The RM scheme should be robust enough to identify and deselect a questionable unit but not deselect a good unit. BIT/BITE indicators in navigation units evolve over long periods and have a heritage going back decades to previous products. Particular indicators are often added to help address certain problems encountered.

    Over the years, corporate knowledge loss results in a manufacturer no longer knowing why a particular indicator is present in the output or what its significance is. Of particular importance are what values performance indicators (e.g., figure of merit) are initialized to after a unit power cycle or re-initialization.

    Unlike aircraft, the Space Shuttle performs BIT on navigation units during flight. Mission Control must understand how to interpret negative results. Does a certain failure indication from BIT always mean that the unit should not be used? Could the unit continue to be used for navigation with no degradation in performance? Nuisance indicators need to be identified and ignored. A BITE masking capability is particularly useful.

    While redundancy management is important, it is not a substitute for well-documented and fully verified software.

22. Do not totally rely on the vendor for navigation expertise. Vendors can provide valuable information on the design, integration, and use of their products. However, they may not always fully understand the applications where their products are used. Users and integrators must maintain navigation expertise to conduct testing, resolve issues, avoid "false pulls" of healthy units that are assumed to be malfunctioning, determine how best to integrate a unit, and provide management with advice on what navigation products are suitable for an upgrade.

    Navigation vendors, who are doing business in a highly competitive market, do not want skilled technical personnel tied to one project for periods of years. The use of a COTS navigation product should not lead one to believe that technical expertise can be "bought" as a COTS product.

23. The ICD is VERY important. If the integrator and user lack access to firmware and firmware requirements, the ICD may be the only written source of information on unit parameters. Developers of software that will interface with the unit must examine the ICD closely. The ICD and the interfacing software must be compared to each other throughout a project. The ICD should also be compared to ground and test results to ensure that it accurately reflects unit input, output and operation. An inaccurate ICD will lead to software and procedural issues that will have to be addressed before a system can be certified as operational. An accurate ICD is also needed for instrumentation port data that is critical during the test and verification phase of a project.

    Understand operation of the box as much as possible before defining requirements for code that will interface with the box. "Bullet proof" the interface since it may not be possible to account for all forms of anomalous unit behavior.

    Some issues encountered on both the MAGR/S, SIGI and relative GPS projects concerned time homogeneous data. Integrators should confirm with the manufacturer which data messages are or are not time homogeneous. This information should be included in the ICD. Non-time homogeneous data makes data analysis and problem resolution more difficult.

    Short development schedules may result in changes to the ICD while host vehicle software requirements are being defined and software is in development and test. A disciplined process of checks must be in place to ensure that the ICD and software requirements for units that interface with the GPS receiver or EGI are consistent. Individuals who have knowledge of both receiver or EGI requirements and requirements for other interfacing units must be able to communicate and be involved in any changes made to the ICD.

24. Knowledge capture. Aviation navigation units often lack detailed, accurate documentation that can be accessed by the integrators and users. If such documentation exists, it is often not included in a contract. The manufacturer may consider some information that would be contained in such documentation proprietary. Much information about unit design and operation possessed by integrators and users is "oral tradition" or "techno-folklore." Different individuals on a project may have conflicting ideas about how a unit works. This can lead to mistakes during integration and difficulties in resolving anomalies from flight and lab tests. Integrators and users should record information about unit operation and design in a "living document" as information is learned from testing and interaction with the vendor. Once design and procedural details are on paper, they can be more easily verified and passed

on to other personnel later. Such a process facilitates the dissemination of accurate information about the unit. Introduction of proprietary data into the document should be avoided.

25. Document the theory behind navigation algorithm requirements. Software requirements documents contain equations to be used, but rarely provide insight into how the equations were derived or how values of constants were determined. This information exists on paper at some point, in the form of informal memos and company internal letters. However, over time, this information is lost due to employee attrition, clean-out of offices, retirements and corporate takeovers. Many mathematical results used in navigation algorithms do not exist in the open literature. Corporate knowledge loss makes it difficult for engineers to understand, evaluate, and modify software years or decades after it was written and certified. Trying to re-derive results can take a considerable amount of time.

    Theoretical development of algorithms should be contained in a configuration-controlled, companion document to the software requirements. The document should be as self-contained as possible, and avoid references to internal letters, informal memos, and presentations that could easily become lost over time. Derivations should include all steps and details of simplifying assumptions. The document should be written for a future engineer in his or her 20s, who possesses a bachelor's degree and who does not have the help of a mentor who understands the material.

26. GPS receivers are complex; firmware quality is important. GPS receivers are computers with tens or hundreds of thousands of lines of code. Like other computers, code errors exist that may not always manifest in a predictable or easily observable fashion. Software bugs can also lie dormant for years until the right set of conditions causes them to manifest.

    Most GPS receivers are equipped with an "autonomous reset" feature to recover from software anomalies. However, receiver resets and software bugs will result in a "loss of service" and make needed data unavailable. Reliability is not just a concern with GPS hardware, it is also a concern with GPS receiver firmware. GPS receivers originally designed for space applications have suffered from significant, though eventually solvable, firmware problems. Even inexpensive handheld GPS units are not immune to technical problems. One popular, low-cost (~$100) unit introduced in 1999 had 10 firmware versions in its first year of production.

    Time critical activities such as atmospheric entry and landing (e.g., Space Shuttle, Crew Return Vehicle), orbital adjustment maneuvers, windows of ground tracking station access, rendezvous, proximity operations and docking require accurate states in a timely manner. Loss of service is also a concern for aviation GPS receivers during final approach. Some NASA spacecraft that use GPS to obtain high position accuracy mandate a rate of software resets to recover from software anomalies of less than one per day. A firmware issue that has "no impact" in an aviation application may require a code fix in an unmanned or manned spacecraft application with high reliability and autonomy requirements.

    An interesting study was recently published concerning the performance of stand-alone aviation GPS receivers that meet Technical Standard Order (TSO) C-129 requirements. The study found that the probability of a receiver outage (loss of service) due to a firmware problem was higher than a signal in space problem that RAIM is designed to detect and deal

with. Although a great deal of effort has been spent on improving GPS accuracy through differential methods, and protecting against signal-in space problems using systems like the Wide Area Augmentation System (WAAS) and the European Geostationary Navigation Overlay System (EGNOS), little attention has been paid to ensuring GPS receiver availability by having quality receiver firmware. The study also concluded that more attention should be paid to characterizing GPS receiver failure probability and failure modes. The Shuttle Program's experience with GPS and EGI units confirms these findings.

27. Lessons learned from other programs. A number of reports have been published recently highlighting the challenges of COTS products used in spacecraft and DoD systems and analyzing failures of unmanned spacecraft, some of which used COTS and a FBC approach.

    Shuttle personnel reviewed these reports for any lessons learned that could have applied to the MAGR/S and SIGI projects. For completeness, some issues identified by those reports are summarized below. Not all of the issues are relevant to the Shuttle navigation upgrade effort.

    - Software development process not well defined, documented, or understood.
    - Contract consolidation led to corporate knowledge loss concerning critical systems.
    - Lack of IV&V.
    - Inadequate communication among project participants.
    - Lack of management involvement and oversight.
    - Inadequate spacecraft monitoring and procedural errors by operators.
    - Navigation equipment not well understood.
    - Spacecraft operators not familiar with system design, operation, and failure modes.
    - Lack of a formal, disciplined process for documenting, advertising, and resolving issues.
    - Inadequate staffing and training.
    - Legitimate issues ignored and attributed to resistance to a "new way" of doing business.
    - Frequent turnover of management and technical personnel.
    - Issues ignored due to cost and schedule pressure.
    - Roles and responsibilities not defined.
    - Technical risks not identified and managed.

28. Provide guidelines for COTS and FBC implementation. A key lesson from unmanned spacecraft failures and DoD software programs is that one must understand how to properly use COTS products and apply FBC principles.

    Some projects have failed since management was not given guidance concerning how to implement a FBC approach. "Faster" and "cheaper" are easily understood, but "better" is difficult to define. This has also led to inconsistent application of FBC principles from one project to another.

    A COTS policy is needed to help prevent cost, schedule, and technical difficulties from imperiling projects that use COTS. Criteria for determining whether a COTS approach can be taken must be determined. Of prime importance is defining the level of insight needed into vendor software, software maintenance, and certification processes.

    Problems in COTS projects can arise when requirements are levied on the product that the vendor did not originally intend the unit to meet. Using COTS may mean either

compromising requirements on the unit or the integrated system. Whether new requirements have to be applied to the unit is a critical decision. Unfortunately, new requirements may not be recognized until the COTS product experiences difficulties in the testing and integration phases of the project.

The Shuttle Program created COTS/MOTS software guidelines for varying levels of application criticality. This recommended policy defines what considerations should be made before deciding to procure a COTS/MOTS product. The following should be examined based on the criticality (impact of failure on safety of flight or mission success) of the application and product in question.

Certification Plan – How much of the vendor's in-house certification can be relied upon? For critical applications, additional testing will be needed if access to test results, source code, and requirements documents is not available. Can the unit be certified to a level commensurate with the criticality of the application?

Vendor Support – This should cover the certification process and the system life cycle. The level of support should be defined based on the criticality of the system.

Product Reliability – Vendor development and certification processes for both hardware and software should be examined.

Trade Studies – Define "must meet," "highly desirable" and "nice to have" requirements. Ability of the unit to meet those requirements, and at what cost, will be a major deciding factor in the COTS decision. Identify loss of operational and upgrade flexibility as well as technical risks and cost associated with the product. Examine the impact of the product on the integrated system, including hardware and software interface changes. Compare the proposed COTS products to a custom developed product. Assess life expectancy of the product and its track record in the market place.

Risk Mitigation – Identify areas that increase risk, such as lack of support if the vendor goes out of business or the product is no longer produced. Ensuring vendor support over the product life cycle can mitigate risk, along with gaining access to source code, design requirements, verification plans, and test results. Off-line simulations of the product should also be considered. Can access be obtained to vendor information on product issues discovered by other users?

Trade studies and risk identification must be performed before committing to the use of a particular unit and integration architecture.

29. Successful application of a COTS EGI. Prototype X-38 vehicles were dropped from a NASA B-52B at Edwards AFB to test the landing guidance, navigation, control and parafoil systems. These vehicles used a COTS EGI unit. The integration and operation of the EGI in the X-38 atmospheric flight tests was smoother than the Space Shuttle, ISS, and CRV projects to use a SIGI unit in Earth orbit. The key to the X-38 drop test success with a COTS EGI was that the EGI was being used in an atmospheric application similar to the application for which it was originally designed. However, as with the Shuttle MAGR/S and Shuttle, ISS and CRV SIGI projects, lack of design insight was an issue.

30. Impact of COTS disappointments. In the last 10 years, inexpensive, accurate navigation devices based on GPS have become available to the public, business and military. News

media reports frequently highlight the “revolution” and “glowing success” stories resulting from GPS technology. Some who do not have a background in navigation take the existence of $100 handheld GPS units to mean that applying GPS technology to an aircraft or spacecraft is as easy as buying a handheld unit at a sporting goods store.

Applying GPS to new applications, such as spacecraft, is not always straightforward. Naiveté about GPS complexity and how applications differ can lead to unrealistic schedule, budget, and technical success expectations. The assumption that the success of terrestrial GPS receivers translates into “cheap and easy” GPS for space applications has actually retarded the maturing of GPS products for space use.

COTS projects that encounter significant technical problems, budget overruns, and schedule slips are “COTS disappointments.” These experiences cause engineers and managers to become suspicious of the technology represented by the COTS product. The problem is not with the technology (e.g., GPS or strapdown navigation) but with the unrealistic expectations attached to COTS projects. These expectations are based on a lack of understanding about the original design and application of the product in question. COTS products are proven devices only when used in the applications for which they were originally designed. The vendors met the contractual obligations of the original customer. The issue is not the technology, or the use of a COTS product, but rather how that technology was applied to meet the needs of the original customer.

The political and budgetary climate may demand a COTS solution, but initial problems using a certain technology can lead to reluctance to work with that technology in the future, particularly in a COTS project. The result is that engineers and management may be reluctant to upgrade to newer technology.

31. Orbit determination accuracy. While accuracy of COTS navigation units may be sufficient in some cases to support low accuracy space flight requirements, Shuttle flights of these units indicate that they are not appropriate for future applications with more demanding orbit determination needs.

    These applications include replacement of ground tracking, satellite formation flying, rendezvous, proximity operations and docking. Some scientific applications, such as determination of atmospheric profiles using GPS signal occultation, have stringent orbital accuracy requirements (1 meter position, 0.1 millimeters/second velocity).

    Formation flying, elimination of ground tracking and orbital replenishment (rendezvous, proximity operations and docking) will place stringent demands on orbit determination and relative navigation accuracy. Firmware quality, hardware reliability and orbit determination accuracy requirements to support these applications will be more demanding than the capabilities of current GPS units. Autonomous, on-board, real-time navigation, relative navigation and burn targeting requires investment in spacecraft navigation systems that will differ from atmospheric flight navigation systems.

32. Velocity accuracy is important. Targeting algorithms that compute precise orbital adjustments to support activities such as (but not limited to) formation flying, rendezvous, proximity operations and docking/grapple need accurate velocity as well as position. Such algorithms have to predict vehicle state vectors into the future over a period of time that may

range from minutes to weeks. Even small velocity errors can result in large position and velocity errors after a prediction using high fidelity integrators and environment models. How well a navigation unit state vector "predicts" the future is a key question that potential users of a unit must ask and address during flight and lab test evaluation.

33. Orbital semi-major axis. A metric used to evaluate how well a state vector will predict is the semi-major axis accuracy. Orbital semi-major axis is a function of position, velocity and energy (1). It is also related to the period of the orbit (2).

$$a = \left[\frac{2}{|\bar{\mathbf{r}}|} - \frac{|\bar{\mathbf{v}}|^2}{\mu} \right]^{-1} = \frac{-\mu}{2E} \qquad (1)$$

$$T_p = 2\pi \sqrt{\frac{a^3}{\mu}} \qquad (2)$$

[D]

Relative semi-major axis accuracy is a good parameter for judging the accuracy of a relative GPS algorithm for formation flying and rendezvous applications.

A recent paper addresses the importance of semi-major axis accuracy and the need for realistic correlation between position and velocity. This paper was written in response to the poor navigation performance observed on Shuttle flights of off-the-shelf GPS receivers and EGIs.

34. Most space navigation conference papers do not address high-accuracy orbit determination. Some papers appearing in the literature advocate geometrical, kinematic type position-determination techniques using GPS data. The advent of all-in-view receivers supports this trend. Such algorithms take advantage of continuous, high-rate GPS measurements and improved measurement geometry compared to ground based radar tracking. From a software perspective, these algorithms are more straightforward since complex environment models (e.g., gravity and drag) are not used. While the position and time data resulting from kinematic positioning algorithms are very accurate and meet the requirements of some missions, this solves only half the problem for other users.

    Many papers discuss a range of space applications of GPS and the high-position accuracy it offers, but pay little or no attention to the need for accurate velocity and semi-major axis estimation. Numerical results of algorithms designed to improve spacecraft navigation accuracy are exclusively focused on position accuracy, with no mention of velocity and semi-major axis errors. Challenges in space-borne applications of GPS are often detailed, such as:

    - Widening the Doppler shift window.
    - Installing an orbit propagator to facilitate reacquisition after a GPS outage.
    - Multipath GPS satellite visibility as a function of spacecraft attitude.
    - GPS satellite visibility to antennas on spinning spacecraft.
    - Increased number of satellites visible on-orbit.

- Satellite visibility and signal strength for geostationary satellite applications.
- Modifying legacy navigation algorithms to accommodate higher orbital altitudes and velocities.

However, the need to improve navigation and filtering algorithms to enhance velocity and semi-major axis accuracy is rarely mentioned. Lack of orbital and relative semi-major axis accuracy data, along with position and velocity correlation data, make it difficult to evaluate the usefulness of relative GPS navigation studies and algorithms published in the literature. Such data is required to assess navigation accuracy impacts on targeting and guidance algorithms and perform propellant budgeting.

35. Receiver specifications. Receivers have specifications for expected position and velocity accuracy under the best tracking conditions. Even receivers designed for space lack a semi-major axis specification. This, coupled with the proprietary nature of receiver firmware, makes it difficult for potential users to determine how suitable a receiver may be for a space application.

    Navigation units that are needed to support advanced concepts (formation flying, rendezvous, autonomous operation, limited ground support and infrastructure) require navigation algorithms that reflect orbital mechanics. While it is true that position, velocity and orbital parameter accuracy requirements vary from program to program, this should not be used to justify a lack of appropriate navigation algorithm missionization.

For Further Information:

Goodman, John L., "Lessons Learned From Flights of 'Off the Shelf' Aviation Navigation Units on the Space Shuttle," Joint Navigation Conference, Orlando, Florida, May 6-9, 2002.

Goodman, John L., "GPS In Earth Orbit – Experiences From the Space Shuttle, International Space Station And Crew Return Vehicle Programs," Proceedings of the 2002 Core Technologies for Space Systems Conference, Colorado Springs, CO, November 19-21, 2002. See http://www.spacecoretech.org/, Technology Maturation, Transfer, and Utilization Session.

Goodman, John L., "The Space Shuttle and GPS – A Safety-Critical Navigation Upgrade," Springer-Verlag Lecture Notes in Computer Science Volume 2580: Proceedings of the 2nd International Conference on COTS-Based Software Systems, Ottawa, Canada, February 10-12, 2003.

Goodman, John L., "A Software Perspective On GNSS Receiver Integration and Operation," Proceedings of the International Space University Conference on Satellite Navigation Systems: Policy, Commercial and Technical Interaction, International Space University, Strasbourg, France, May 26-28, 2003, published by Kluwer Academic Publishers, Dordrecht, The Netherlands, 2003.

Evidence of Recurrence Control Effectiveness:

N/A

Documents Related to Lesson:

NPR 7120.5, "NASA Program and Project Management Processes and Requirements"

Mission Directorate(s):

Exploration System

Aeronautics Research

Space Operations

Additional Key Phrase(s):

Administration/Organization

Communication Systems

Computers

External Relations

Flight Equipment

Flight Operations

Independent Verification and Validation

Information Technology/Systems

NASA Standards

Policy & Planning

Procurement, Small Business & Industrial Relations

Research & Development

Risk Management/Assessment

Safety & Mission Assurance

Software

Spacecraft

Standard

Test & Verification

B-23. Public Lessons Learned Entry: 1480

Lesson Info:

- Lesson Number: 1480
- Lesson Date: 2004-06-21
- Submitting Organization: JPL
- Submitted by: Mark Boyles/David Oberhettinger

Subject:

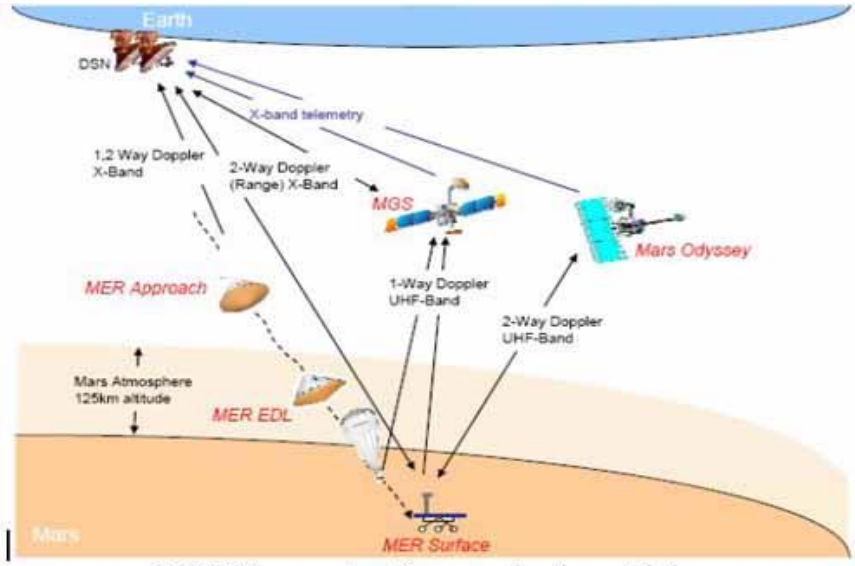
Provide In-flight Capability to Modify Mission Plans During All Operations (2004)

Abstract:

The Mars Exploration Rover (MER) flight system had the ability to update EDL parameters during Approach, and the mission design furnished an operational plan, process, and tools for performing the updates. These capabilities permitted JPL to respond to new data on the Mars atmospheric density by modifying the timing of the MER parachute release, assuring mission success. Maintain an operational capability to code critical parameters in FSW and to update them during the latter stages of encounter/EDL.

Description of Driving Event:

Both the MER flight system and mission designs had the flexibility to react to unexpected events. The MER flight system provided an in-flight capability to revise EDL parameters by coding them in flight software. The MER mission design provided an operational plan, process, and tools permitting JPL to perform EDL parameter updates over a span of several days during final approach to Mars and up to six hours before landing.



MER Encounter Communications Links

The ability to update EDL parameters was critical to the success of the MER mission. Updated data on Martian atmospheric pressure received from the Thermal Emission Spectrometer instrument on the MGS spacecraft during final approach (see figure) indicated a lesser atmospheric density than expected. Left uncorrected, the actual lesser atmospheric density could

have caused MER to sense its dynamic pressure target at a lower altitude than planned, and to trigger its parachute deployment too near the ground. Because the flight team had the processes for changing EDL parameters, and the ability to modify these parameters after launch, the timing of the MER parachute release was accomplished.

References:

1. "Mars Exploration Rover (MER) Flight Operations Report," NESC Report No. RP-04-04/03-004-I.
2. 2003 Mars Exploration Rover Final Navigation Peer Review, February 3, 2003.

Additional key words: Mars lander, Mars probe, mission failure, signal loss, flight constraints, communications lag, continuous telemetry

Lesson(s) Learned:

Critical parameters coded in FSW and the ability to alter them within hours of critical events in response to unexpected data on flight characteristics can save a planetary mission or deep space encounter.

Recommendation(s):

For spaceflight missions—particularly landers—ensure that the flight system and mission designs have flexibility to react to unexpected events:

1. Code-critical parameters in flight software.
2. Maintain an operational capability to update these parameters during the latter stages of encounter/EDL.

Evidence of Recurrence Control Effectiveness:

Corrective Action Notice No. Z84232 was opened by JPL on July 6, 2004 to initiate and document appropriate Laboratory-wide corrective action on the above recommendation.

Documents Related to Lesson:

JPL Procedure: Mission Planning-Operations, JPL Document 31912, March 05, 1999.

NPR 7120.5, NASA Program and Project Management Processes and Requirements.

Mission Directorate(s):

Exploration Systems

Aeronautics Research

Additional Key Phrase(s): Communication Systems, Environment, Flight Equipment, Flight Operations, Hardware, Payloads, Risk Management/Assessment, Safety & Mission Assurance, Spacecraft

Appendix C. GN&C-Related Best Practices from the NASA GSFC GOLD Rules Database

Subsection	GOLD Rule	Subject
1	1.17	Safe Hold Mode
2	1.07	End-to-End Phasing
3	1.33	Polarity Checks of Critical Components
4	1.32	Thruster & Venting Impingement
5	1.31	Actuator Sizing
6	1.30	Controller Stability Margins
7	1.19	Initial Thruster Firing Limitations
8	1.22	Purging of Residual Test Fluids
9	1.24	Propulsion System Safety Electrical Disconnect

1. GSFC GOLD Rule 1.17: Safe Hold Mode

Abstract

All spacecraft shall have a power-positive control mode (safe hold) to be entered in spacecraft emergencies. Safe Hold Mode shall have the following characteristics:

1. Its safety shall not be compromised by the same credible fault that led to safe hold activation.
2. It shall be as simple as practical, employing the minimum hardware set required to maintain a safe attitude.
3. It shall require minimal ground intervention for safe operation.

Significance

Safe Hold Mode should behave very predictably while minimizing its demands on the rest of the spacecraft. This facilitates the survival, diagnosis, and recovery of the larger system. Complexity typically reduces the robustness of safe hold, since it increases the risk of failure due to existing spacecraft faults or unpredictable controller behavior.

Details

Pre-Phase A Concept Studies

1. Ensure that requirements document and operations concept include Safe Hold Mode.
2. Verify through peer review and at MCR.

Phase A Preliminary Analysis

1. Ensure that requirements document and operations concept include Safe Hold Mode.
2. Verify through peer review and at MDR.

Phase B Definition

1. Identify hardware & software configuration for Safe Hold Mode.
2. In preliminary FMEA, demonstrate that no single credible fault can both trigger safe hold entry and cause safe hold failure.
3. Analyze performance of preliminary safe hold algorithms.
4. Verify through peer review and at PDR.

Phase C Design

1. Establish detailed safe hold design including entry/exit criteria and FDAC requirements for flight software.
2. In final FMEA, demonstrate that no single credible fault can both trigger safe hold entry and cause safe hold failure.
3. Analyze performance of safe hold algorithms.
4. Via a rigorous risk assessment, decide whether to test safe hold on-orbit.
5. Verify through peer review and at CDR.

Phase D Development

1. Implement Safe Hold Mode.
2. Verify proper mode transitions, redundancy, and phasing in ground testing.
3. Execute recovery procedures during mission simulations.
4. Perform on-orbit testing if applicable.
5. Verify at PER and FOR.

Resources

During Phase C, a simulation environment should be established that allows FSW and hardware and ground system elements to be easily swapped in and out. This HITL simulation is used for end-to-end testing.

2. GSFC GOLD Rule 1.07: End-to-End GN&C Phasing

Abstract

All GN&C sensors and actuators shall undergo end-to-end phasing/polarity testing after spacecraft integration and shall have FSW mitigations to correct errors efficiently.

Significance

Many spacecraft have had serious on-orbit problems due to inadequate verification of signal phasing or polarity. Component-level and end-to-end phasing tests and FSW mitigations can ensure correct operation.

Details

Phase B Definition

1. Define interface requirements of sensors and actuators.

2. Design FSW to include capability to fix polarity problems via table upload.

3. Verify through peer review and at PDR.

Phase C Design

1. Update ICDs to include polarity definition.

2. Review vendor unit-level phasing test plans.

3. Write FSW to include capability to fix polarity problems via table upload.

4. Create unit-level and end-to-end phasing test plans.

5. Verify through peer review and at CDR.

Phase D Development

1. Perform unit-level phasing tests.

2. Test FSW for table upload functionality.

3. Perform end to end phasing test for all sensor-to-actuator combinations.

4. Develop & test contingency flight ops procedures for fixing phasing problems.

5. Verify at PSR and LRR.

Resources

During Phase C a simulation environment should be established that allows FSW and hardware and ground system elements to be easily swapped in and out. This HITL simulation is used for polarity testing.

3. GSFC GOLD Rule 1.33: Polarity Checks of Critical Components

Abstract

All hardware shall be verified by test or inspection of the proper polarity, orientation, and position of all components (e.g., sensors, switches, and mechanisms) for which these parameters affect performance.

Significance

Each spacecraft and instrument contains many components that can be reversed easily during installation. Unless close inspections are performed, and proper installations are verified by test, on-orbit failures can occur when these components are activated.

Details

Phase A Preliminary Analysis

1. Identify all polarity-dependent components in the spacecraft design concept.
2. Ensure that design concept provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level.
3. Verify through peer review and at MDR.

Phase B Definition

1. Identify all polarity-dependent components in the spacecraft prelminary design.
2. Ensure that preliminary design provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level.
3. Develop test plan for polarity-dependent components.
4. Verify through peer review and at PDR.

Phase C Design

1. Identify all polarity-dependent components in the spacecraft detailed design.
2. Ensure that detailed design provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level.
3. Develop test procedures for polarity-dependent components.
4. Verify through peer review and at CDR.

Phase D Development

1. Execute polarity tests at subsystem and end-to-end mission system levels.
2. Verify at PER and PSR.

Resources

During Phase C a simulation environment should be established that allows flight S/W and H/W and ground system elements to be easily swapped in and out. This HITL (Hardware In The Loop) simulation is used for polarity testing.

4. GSFC GOLD Rule 1.32: Thruster and Venting Impingement

Abstract

Thruster or external venting plume impingement shall be analyzed and demonstrated to meet mission requirements.

Significance

Impingement is likely to contaminate critical surfaces and degrade material properties. It can also create adverse and unpredictable spacecraft torques and unacceptable localized heating.

Details

Phase B Definition

1. Develop analytical mass transport model.

2. Update model as design evolves.

3. Verify at PDR.

Phase C Design

1. Refine analysis based on updated designs.

2. Verify at CDR.

Phase D Development

1. Refine analysis based on updated designs.

2. Measure venting rates during T/V tests and verify analysis.

3. Verify at PSR.

Resources

The hot fire test of thrusters during T/V of a spacecraft is not possible because it is not safe for personnel and would destroy/contaminate both the T/V test equipment and the spacecraft. Plume testing is done at the thruster level, which would require a high-altitude hot-fire test facility and equipment capable of measuring the plume flow field. Typically, the plume mass transport models used in the industry have been previously verified against hot-fire test data, which eliminates the need for further testing at the spacecraft level.

5. GSFC GOLD Rule 1.31: Actuator Sizing Margins

Abstract

The ACS actuator sizing shall reflect specified allowances for mass properties growth.

Significance

Knowledge of spacecraft mass and inertia can be uncertain at early design stages, so actuator sizing should be done with the appropriate amount of margin to ensure a viable design.

Details

Phase A Preliminary Analysis

1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 100% design margin.
2. Verify at MDR.

Phase B Definition

1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 50% design margin.
2. Verify at PDR.

Phase C Design

1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 25% design margin.
2. Verify at CDR.

Resources

None.

6. GSFC GOLD Rule 1.30: Controller Stability Margins

Abstract

Controller designs shall meet or exceed minimum gain and phase margin requirements as specified below.

Significance

Proper gain and phase margins are required to maintain stability during reasonable unforeseen changes in spacecraft configuration or control system parameter values.

Details

Phase A Preliminary Analysis

1. The ACS concept shall identify whether the gain and phase margin requirements will be difficult to meet due to the spacecraft configuration.
2. Verify through peer review and at MCR and MDR.

Phase B Definition

1. The ACS controller rigid body gain and phase margin shall be designed to meet the requirement of 12 db and 30 degrees respectively.
2. Verify through peer review and at PDR.

Phase C Design

1. The ACS controller flexible body gain and phase margin shall be designed to meet the requirements of 6 dB and 30 degrees, respectively. Use gain attenuation methods only. Phase attenuation methods should not be used.
2. Verify through peer review and at CDR.

Resources

COTS stability analysis software.

7. GSFC GOLD Rule 1.19: Initial Thruster Firing Limitations

Abstract

All initial thruster firings shall occur with real-time telemetry and command capability. If alternate actuators (e.g., reaction wheels) are present, the momentum induced by initial firings shall be within the alternate actuators' capability to execute safe recovery of the spacecraft.

Significance

Polarity issues and thruster underperformance typically occur early in the mission. Both conditions can result in a spacecraft emergency due to excessive spacecraft spin rates.

Details

Pre-Phase A Concept Studies

1. The ACS concept shall ensure that thrusters will not be required during launch vehicle separation for a 3-sigma distribution of cases. The concept for operations shall ensure that, except in case of emergency, all thrusters can be test fired on-orbit prior to the first delta-v maneuver.
2. Verify through peer review and at MCR.

Phase A Preliminary Analysis

1. The ACS shall design the thruster electronics, size and place the thrusters, and size other actuators (e.g. reaction wheels) such that a failed thruster can be shut down and the momentum absorbed before power or thermal contstraints are violated. The activities specified in Pre-Phase A shall be maintained.
2. Verify through peer review and at MDR.

Phase B Definition

1. Hardware (e.g., processors, power interfaces, data interfaces) and software shall ensure that anomalous thruster firings will be shut down quickly enough to allow recovery of the spacecraft to a powersafe and thermal-safe condition.
2. Develop design and operations concept consistent with the activities established in Pre-Phase-A.
3. Verify through peer review and at PDR.

Phase C Design

1. Establish detailed recovery procedures. Finalize design and operations concept consistent with the activities established in Pre-Phase-A.
2. Verify through peer review and at CDR.

Phase D Development

1. Test failed thruster conditions with the greatest possible fidelity. Verify transitions and polarity.
2. Ensure that recovery procedures have been simulated with the flight operations team.

3. During on-orbit testing, thrusters shall be test fired to verify polarity and performance prior to being used in a closed loop control.
4. GN&C and system engineering organizations shall verify at SAR.
5. Follow-up at ORR.

Phase E/F Operations and Disposal

1. Ground contact shall be maintained during thruster firings.

Resources

None.

8. GSFC GOLD Rule 1.22: Purging of Residual Test Fluids

Abstract

Propulsion system design and the assembly and test plans shall preclude entrapment of test fluids that are reactive with wetted material or propellant.

Significance

Residual test fluids can be reactive with the propellant or corrosive to materials in the system leading to critical or catastrophic failure.

Details

Phase B Definition

1. If test fluids are used in the assembled system, present plans for purging and drying of the system.
2. Verify at PDR.

Phase C Design

1. Demonstrate that the method for drying the wetted system has been validated by test on an equivalent or similar system.
2. Verify at CDR.

Phase D Development

1. Verify dryness of wetted system by test.
2. Verify at PSR.

Resources

If portions of a propulsion subsystem are exposed to cleaning and test fluids, the lines, tanks, and components must be dried by some process that usually requires alternating between dry-gas purging and hot-vacuum drying. Whatever the process, the verification of dryness is required. For water, the use of a dewpoint analyzer is sufficient to verify dryness. For other types of fluids, vapor chemical analyzers of some type that measure parts per million (ppm) will be required.

9. GSFC GOLD Rule 1.24: Propulsion System Safety Electrical Disconnect

Abstract

An electrical disconnect “plug” or set of restrictive commands shall be provided to preclude inadvertent operation of components.

Significance

Unplanned operation of propulsion system components (e.g., dry cycling of valve, heating of catalyst bed in air, firing of thrusters after loading propellant) can result in injury to personnel or damage to components.

Details

Phase B Definition

1. Present design and/or operational plan that precludes unplanned operation of propulsion system components.
2. Verify at PDR.

Phase C Design

1. Present detailed design of electrical disconnect and/or set of restrictive commands to preclude unplanned operation of propulsion system components.
2. Verify at CDR.

Phase D Development

1. Demonstrate the effectiveness of the disconnect and/or set of restrictive commands by test.
2. Verify at PER.

Resources

During CDR, the disconnect or disabling plug design and its operational verification should be presented. If a simple visual inspection of design is not sufficient verification of functionality, then a verification test will be required. Depending on the extent of the test, some or all of the following test equipment will be required: disable and enable plugs, ohm and voltage meters, power source, and a flight wire harness mock-up complete with a thruster valve driver or simple electrical switch and a thruster mated to the wire harness with either plug installed (the enable plug is used to verify the functionality of the test mock-up then the disable plug is installed to verify its capable of disabling the thruster).

Appendix D. GN&C-Related Lessons Learned Extracted from the Aerospace Corporation Document, "100 Questions for Technical Review"

(Aerospace Report No. TOR-2005(8617)4204

Lesson #	Subject
2	Perform Independent Mass Property, Stability Control and Structural Load Analyses on Spacecraft
13	Flexible Solar Arrays Are Susceptible to Thermally Induced Vibrations
18	Spacecraft Structure Dynamical Interaction with Attitude Control
27	Control Propellant Balance
29	Validate Changes in Command Script Configuration
33	Check Satellite-Launcher Compatibility As Early As Possible
35	Implement Independent Fault Protection
36	Implement Independent Fault Protection (II)
43	Do Not Circumvent Processes Designed to Catch Human Errors
53	Test Hardware and Software Together (Polarity Tests)
60	Tests Are for Verification, Not Discovery (Polarity Tests)
73	Trace All Software Changes Back to System Requirements
80	Check, Double-Check, and Triple-Check Torquer Phases (Polarity Tests)
97	Control Hardware and Software Configuration Before, During, and After Tests

2

Perform Independent Mass Property, Stability Control, and Structural Load Analyses on Spacecraft and Launch Vehicles

The Problem:

Mistakes in determination of mass-property and control-stability analyses have caused a large number of launch failures. Examples include:

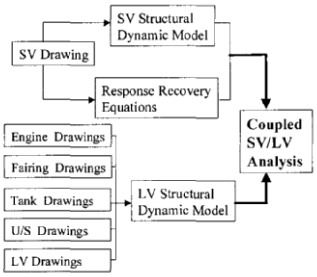
- Inappropriate reuse of aerodynamic coefficients (1994).
- Unanticipated structural vibration mode not filtered out (1995).
- Incorrectly simulated weight (1995).
- Underprediction of the load as well as an unexpected resonance due to wind shear (1992 and 1995).
- Unexpected increase in horizontal velocity (1996).
- Unaccounted roll mode caused by air-lit solid rocket motors (1998).

Flawed analysis has also led to numerous on-orbit anomalies.

The Cause:

Launching a satellite calls for extremely complex simulation of the mass, thermo-structural, fluid-mechanical, propulsion, and control properties (a single subsystem can easily involve over 100,000 equations). The state of the art in this area is far from robust: subtle assumptions, insufficiently sophisticated techniques, or human errors can all throw the results seriously off.

Moreover, when the satellite is integrated with the launcher, each organization must generate parochial models but each has little insight into each other's analytical process. Costly problems can easily arise without a clear settling of responsibility, especially with today's emphasis on proprietary data protection.



Integrating space vehicle (SV) to launch vehicle (LV) involves complex modeling; independent analysis is often necessary to overcome organizational barriers.

Lessons Learned:

- Inaccuracies on mass property, stability control, and structural loads continue to threaten mission performance.
- To ensure correct analysis, many programs require an independent analysis. These activities also help validate operational procedures, support flight anomaly resolution, and overcome the organizational issues. There have been no catastrophic failures in programs that abide by this policy, and several failures were averted thanks to independent analysis.

For more technical information, call Ray Skrinska at (310) 336-4001.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

13

Flexible Solar Arrays Are Susceptible to Thermally Induced Vibrations

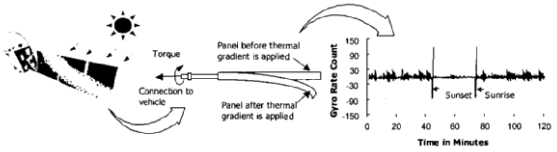
The Problem:

Thermally induced vibrations of spacecraft appendages have recurred numerous times. Resultant problems include:

- Two science satellites stopped spinning (early 1960s).
- Two Earth observation satellites showed large disturbances about the roll and yaw axes whenever the spacecraft entered or exited sunlight (early 1980s).
- A space observatory had to have its solar arrays replaced on-orbit because "jitters" interfered with star pointing (1993).
- A scientific satellite failed due to heating and expansion of the solar panels that damaged the structure (1997).

The Cause:

Spacecraft equipped with long appendages or solar arrays are susceptible to attitude perturbation upon entering or leaving the Earth's shadow, because large temperature gradients can develop around the boom. The sun-facing side of the boom or array can bend and create a torque on the satellite very rapidly, causing a flutter. Satellites with a single solar array are most susceptible.



Long appendages can deform and cause the spacecraft to shiver during eclipse transitions. Effective attitude control algorithms should be developed to address this concern.

The space observatory mentioned above, for example, employed flexible solar arrays with telescoping booms. A thermal gradient as much as 25-deg C developed around the boom circumference within one minute, causing the tip of the spar to defect by 20 cm.

Lessons Learned:

- Flexible solar arrays and supporting equipment are sensitive to thermal environment.
- Thorough thermomechanical analyses of the solar arrays, particularly on their modal frequencies, should be conducted.
- Control algorithms used to mitigate the effects of solar-array excitations should be refined.

For more technical information, call John Welch at (310) 336-6556.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

18

Make Sure Critical Software Performs in its Intended Environment

The Problem:

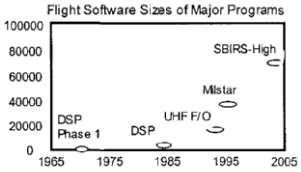
The 1996 maiden flight of a launch vehicle ended in a crash.

The Cause:

The launcher's flight control system, which had derived considerable heritage from the previous generation, used two identical inertial reference controllers, including a "hot" stand-by.

One function inherited from the legacy software computed the platform alignment before launch. This function was no longer needed in the new generation.

The new rocket flew a different trajectory, creating an alignment bias that was too large for the legacy code to compute. An "operand error exception" occurred.



As software takes over many functions that used to be controlled by hardware, code sizes increase almost exponentially. Software reliability thus poses a growing challenge and warrants more quality assurance efforts.

Such errors are common, and are typically handled by software (for example, by inserting "likely" values). Unfortunately, although the programmers did identify the alignment bias input as one of the several variables capable of causing operand errors, they chose to leave it unprotected, probably supposing that there would be large safety margins.

More tragically, the system was designed in the belief that any fault would be due to random hardware problems, and should be handled by an equipment swap. Thus, when the software detected the errant and irrelevant exception, it halted the active controller and switched to the backup. Of course, the backup immediately encountered the same error exception, and also shut down. The launch vehicle in essence destroyed itself even though both controllers worked perfectly.

Lessons Learned:

- Hardware redundancy does not necessarily protect against software faults.
- Mission-critical software failures should be included in system reliability and fault analysis.
- Software specifications should always include specific operational scenarios.
- Software reuse should be thoroughly analyzed to ensure suitability in a new environment, and all associated documentation, especially assumptions, should be reexamined.
- Extensive testing should be performed at every level, from unit through system test, using realistic operational and exception scenarios.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

27

Control Propellant Balance

The Problem:

Dynamic instability caused by fluid imbalance has afflicted several satellites during orbit transfer maneuvers. Example include:

- A commercial communication satellite was stranded in a low orbit, and had to expend significant fuel in hundreds of thruster firings to reach a geosynchronous orbit.
- A foreign satellite failed to reach geostationary orbit.
- A military communication satellite wobbled unexpectedly (but was able to recover).

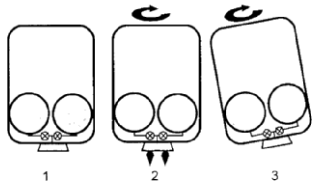
The Cause:

Propulsion control is a delicate task because many parameters, such as the flow rate of propellant in space, cannot be precisely modeled or controlled.

Several factors can trigger fluid imbalance:

- Improper fuel-load procedures. (This problem caused the first incident cited above).
- Differences in flow rates or valve responses can cause propellant to be drawn preferentially from one tank over another. (This problem probably caused the second mishap).

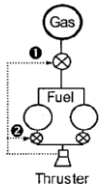
If one tank is cooler than the other, propellant will flow into the cooler tank from the warmer tank, causing imbalance.



As satellites spin during transfer maneuvers, mass imbalances coupled with centrifugal forces can cause tilting. Severe tilt can divert the transfer thrust and prevent satellites from reaching their proper orbit.

Lessons Learned:

- Make sure tank loads are balanced.
- Use a single tank, if feasible, to avoid propellant migration.
- Ensure that attitude-control algorithms and mechanisms can correct dynamic instability caused by propellant imbalance.



Feedback loops can be designed to control gas pressure (❶) or fuel flow (❷) between the tanks to restore balance. The latter method is more precise.

- If possible, place a gas pressure regulator above the tanks, or latching isolation valves below each tank, to control propellant flow.

For more technical information, call Mark Mueller at (310) 336-5081.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

29

Validate Changes in Command Script Configuration

The Problem:

Contact with a deep space observatory was lost (control was regained three months later following a dramatic rescue; see Lesson 30).

The Cause:

The spacecraft used three gyros:

- Gyro A, to control the safe mode;
- Gyro B, to detect faults; and
- Gyro C, for normal attitude control.

The flight software should turn on the normally off Gyro A when the satellite entered safe mode. Unfortunately, the engineer making a command procedure change did not know to implement the enable command. A loose change-control process failed to catch the error.

The Lagrange Points

There are five Lagrange Points where gravitational attractions from the Sun and Earth balance each other. The loss of control occurred at the first Lagrange Point (L1, about 1.5 million kilometers from Earth), from which location the space observatory monitors solar activities. The L2 point, on the night side, is suitable for infrared astronomy.

During a routine operation, Gyro B was accidentally set incorrectly, causing a false reading. The on-board computer detected B's error and put the satellite in safe mode. The fault on B was fixed, but control shifted from C to A.

Sensed rates from Gyro A (despun, reading zero) and B (active with variable readings) soon diverged, prompting the thruster to fire to try to null the nonexistent roll error. The effort was futile, and the satellite entered safe mode again two hours later.

The spacecraft was designed to survive in safe mode for at least 48 hours. Nonetheless, the operators did not pause to analyze why one anomaly followed on the heels of another. Side-stepping the required telemetry data check that would have indicated that Gyro A was in fact off, the operators mistook Gyro B's variable readings as a sign of a fault, and turned it off. With no functional gyro, control was soon lost.

Lessons Learned:

- Treat command-procedure changes with the same rigor as flight-critical software. This includes formal configuration management, peer review with knowledgeable technical personnel, and full command verification with an up-to-date simulator.
- Ensure change implementation timelines are consistent with staff workloads.
- Display spacecraft health and safety information clearly.
- Follow validated operations procedures, including review of all pertinent data.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

33

Check Satellite-Launcher Compatibility As Early As Possible

The Problem:

A technology demonstrator satellite had to be substantially redesigned because the vehicle's stability during the orbit-transfer maneuver was not considered early on.

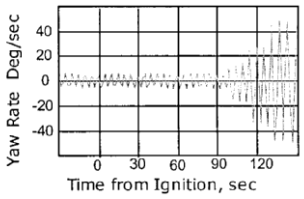
The Cause:

When a satellite spins, its components vibrate at a "nutation frequency" determined by the moments of inertia and by the spin rate. Flexible parts, such as whip antennas and fluids, will dissipate the rotational energy, particularly if these parts resonate near the nutation frequency. Energy dissipation may lead to increased coning angles, even a flat spin.

Nutational growth caused several early satellites to malfunction. Although well understood in general today, it remains a challenge whenever spinning upper stages are used—because fuel motion and burning complicate the analysis, the satellite should be designed with extra margins to prevent the stack from entering a flat spin during orbit transfer.

The upper stage selected by this program spins. Unfortunately, the contractor failed to pay attention to the issue during preliminary design, despite advice from experts. The instability could have been mitigated by simply modifying the satellite propellant tanks. However, because the problem was recognized late, numerous costly modifications became necessary. The project was almost cancelled.

The first American satellite, Explorer 1, went into a flat spin because its flexible antennas triggered nutational growth.



As shown here, solid upper stages, which this mission used, are more prone to instability. The satellite contractor did not recognize this risk in part because the launch vehicle contractor failed to formally communicate this requirement. The design changes kept the instability in check during flight, and the satellite reached the correct orbit.

Lesson Learned:

- Ensure interface problems between the satellite and launcher, such as dynamic instability, are analyzed early on in the design process (see Lessons 2, 11).

For more technical information, call David Stampleman at (310) 336-2243.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

35

Implement Independent Fault Protection

The Problem:

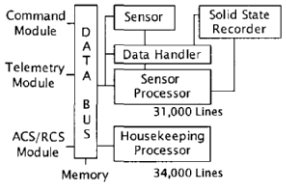
A deep-space mission ended prematurely after excessive thruster firing depleted its fuel.

The Cause:

This spacecraft was developed by a highly motivated group operating under a rigid cost cap and tight schedule. Flying just 22 months after being funded, it successfully circled the moon and demonstrated many technologies.

Soon afterward, however, a maneuver triggered a numeric overflow in the processor, causing it to erroneously fire its thrusters and freeze. A "watchdog timer" algorithm should have stopped the thrusters from continuously firing, but did not execute because the computer had already crashed. By the time ground operators regained control, all the fuel was gone.

A hard-wired timer, which would have stopped thruster firing, was not implemented due to the tight schedule. Time pressure also prevented the software from being fully tested, and many changes had to be uploaded as faults were discovered.



A Rushed Job

Over 65,000 lines of flight code (only 20% inherited) were developed in 17 increments within one year, leaving little time for thorough testing.

The overflow error had occurred thousand of times (without causing malfunctions) because the project had to settle for an inadequate but available processor. Software changes had been written to correct the problem, but the overstretched staff could not handle operations, anomaly analysis, and software repair at the same time, and the change was not loaded.

Four years later, another interplanetary probe encountered a similar anomaly. Fortunately, engineers learned the lessons from the previous incident; the precautions they took allowed them to successfully complete the mission (see Lesson 36).

Lessons Learned:

- Apply independent fault protection for critical software functions.
- Implement exception handling to protect the flight processor from aborts due to data handling errors (see Lesson 18).
- Do not cut corners in testing critical flight software.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

36

Implement Independent Fault Protection (II)

The Event:

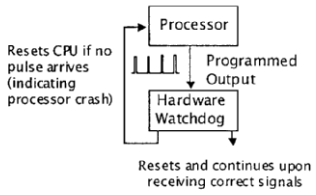
An interplanetary probe recovered from a major anomaly.

The Cause:

The spacecraft, designed to rendezvous with an asteroid, employed extensive autonomy because ground intervention during an emergency would take too long. The designers studied the history of an earlier project, which terminated prematurely after a data error depleted on-board fuel (see Lesson 35).

Three years into the flight, an engine burn aborted. A missing command in the burn-abort contingency command script prevented a graceful transition into the safe mode, and a series of anomalies ensued. Communication was lost for 27 hours before the flight computer regained control.

The initial script error was not caught during software tests. Hardware-in-the-loop simulation could not test abort scenarios because the brassboards were difficult to use. Exactly how the anomalies propagated is unclear because a bus undervoltage wiped out data from the recorder, nor could the anomalous behaviors be reproduced on ground.



Watchdog Scheme (Simplified)

The processor feeds a series of programmed pulses into the hardware timer, which will reset itself and await the next input. If the expected "heartbeat" does not arrive, the watchdog knows that the processor has probably crashed and intervenes (such as by initiating a fault protection routine).

During the emergency, the spacecraft fired its thrusters thousands of times. Fortunately, the fuel loss was tolerable because the thrusters were hardwired to fire only for fractions of a second. The mission was saved because the designers took precaution against fuel depletion during a software crash, a lesson learned from the previous failure.

Lessons Learned:

- Create extensive, realistic nominal and anomalous operational scenarios for testing at every level, from unit through system test.
- Implement robust simulators, including hardware-in-the-loop, for testing critical flight software functions.
- Apply independent fault protection, such as hardware watchdogs, to mitigate risk in real-time systems, where errors can be so deeply buried as to be practically undetectable.

For more technical information, call Richard Adams at (310) 336-2907.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

43

Do Not Circumvent Processes Designed to Catch Human Errors

The Problem:

A satellite was placed into a moderately degraded orbit.

The Cause:

During launch preparations, operators made final measurements of the spacecraft's inertial measurement unit (IMU). The readings, together with factory calibration data, were used to control the satellite's orientation during ascent.

Unlike all the other inputs loaded to the satellites, the IMU measurement and calibration data could not be verified in a testbed because the readings had to be made just before launch. Therefore, a procedure was set forth to avert mistakes: one operator was required to transcribe the calibrations numbers from the factory printout, another would verify the entries.

An engineer supervising the keyboard operators copied the calibration data from the computer printout onto a scratch paper, leaving the original printout in his office. He gave the scratch paper to the operators, telling them that it was suitable. The data were typed in and verified.

Unfortunately, the engineer left out a symbol, and the orbit insertion went awry!

$\dot{R}_n$ versus $\bar{\dot{R}}_n$

The First Software-Related Crash

An incorrect formula in the ground software led to the failure of Mariner I in 1962.

Ascent control required velocity smoothing, or "R dot bar n" where R stood for radius from a tracking antenna, the dot for the first derivative (i.e., the velocity), the bar for averaging, and n for the increment.

The bar was left out of the handwritten equations provided to the programmer, causing the guidance computer to be coded to process raw velocity instead. Confronted by fluctuating telemetry, the computer sent erratic correction signals, forcing a smoothly ascending booster to veer off course.

Lessons Learned:

- Ascertain software databases as thoroughly as the source codes (see Lesson 3).
- Verify software algorithm and database on a simulator whenever possible.
- Double-check manually entered data against original sources.
- Automate data transfer and checking whenever possible to minimize human error.

For more technical information, call Julio Rivera at (310) 336-3287.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

53

Test Hardware and Software Together

The Problem:

A satellite lost power shortly after launch.

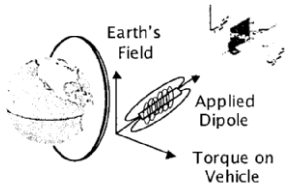
The Cause:

The satellite used magnetic torquers for attitude control, a common approach.

Installation constraints made it necessary to mount one of the torque coils with a phase opposite of that of the other two coils. Unfortunately, this configuration was not reflected in the software reused from another mission, resulting in a sign error.

The mistake was not caught because the software was reviewed only at a top level. Moreover, the attitude control test to verify coil wiring was hardware-only. An end-to-end test, which would have detected the fault, was deemed too costly.

In orbit, the phase reversal caused the solar array to be steered away from the Sun. Limited ground station coverage made it impossible to diagnose the problem soon enough to prevent the battery from being drained.



Magnetic torquers are coils wound around an iron core. Passing a current through the coils creates a magnetic dipole which interacts with the Earth's magnetic field and generates a feeble torque. Reversing the current flow (phase) produces the opposite effect.

Torquer polarity mistakes occur often. The orientation of large coils are easily verified with a magnetometer (essentially a compass). Background noise can make checking small torquers difficult.

Lessons Learned:

- Rigorously control configuration, especially at hardware/software interface.
- Always ascertain torquer polarity.
- Provide sufficient ground station coverage in early operation.
- Design battery protection to keep the satellite alive long enough for troubleshooting by implementing automatic load shedding and by configuring solar panels so that even a partially deployed array could keep battery charged.

For more technical information, call Tom Fuhrman at (310) 336-6596.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

60

Tests Are for Verification, Not for Discovery

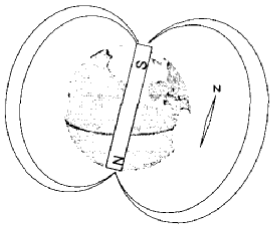
The Problem:

A satellite started to tumble shortly after deployment.

The Cause:

The spacecraft used magnetic torque rods to stabilize body spins. During the Guidance and Control (G&C) subsystem test, an analyst misinterpreted the meaning of the Earth's magnetic poles and set the flight software incorrectly. The error went unnoticed because the coil test had no expected polarity values—the configuration was determined based on the measured responses.

After separating from the launcher, the satellite began to wobble. Fortunately, the lead G&C engineer was prepared. Having heard many horror stories about torque rod phase mistakes, he had spent the previous day making contingency plans. Within half an hour, he reversed the controller gain, stabilizing the satellite.



The Earth as a Magnet

Opposite magnetic poles attract. The north pole of magnet needles points to the Earth's magnetic South Pole, also called the geomagnetic North Pole!

Lessons Learned:

- Expected test results should be established in advance of the test. Deviation from expected results should raise a flag, and be thoroughly investigated before making any changes.
- Rigorously manage software development, especially on requirements, interfaces, and configuration control.
- Plan for contingencies, using a top-down fault tree (ask "what happens if the satellite failed to de-spin?" for example).
- Double-check torquer signs (Lesson 53).

For more technical information, call Tom Fuhrman at (310) 336-6596.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

73

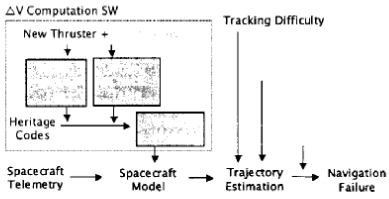
Trace All Software Changes Back to System Requirements and Specifications—Do Not Simply Modify the Code

The Problem:

A spacecraft broke up near Mars.

The Cause:

En route to Mars, the probe would fire its thrusters to unload the reaction wheels. Ground controllers planned the burns with a thruster model, reused from a successful mission.



Complex Failure Causes

A thruster change made it necessary to update this model, which specified thruster input in Newton-sec. The thruster vendor—the same for both missions—used lb-force-sec. In the original model, engineers correctly added the 4.45 conversion factor to the vendor's equation. Overlooking the interface specification and seeing no warning in the code comments, the follow-on team simply made a substitution.

Labeled as non-mission critical, the ground software—without the conversion factor—was not rigorously reviewed; the "truth" table, computed manually for acceptance testing, contained the same mistake. Interface with the navigation function was informally tested only to ensure that it could move across servers.

Only one, occasionally two, engineers navigated the spacecraft. Two months before orbit insertion, radar returns projected a path too close to Mars. Unfortunately, as the probe neared Mars, poor observation geometry from Earth reduced tracking precision. The flight team, confident with their navigation ability, decided against raising the orbit.

Not until aerobraking, after Martian gravity had captured the probe, was it possible to calculate the spacecraft's true position. Only then did the controllers realize the probe was 100 kilometers off course!

The successful reflight listed both English and metric units on all interface control documents, adopted a more robust navigation method, and used six full-time navigators.

Lessons Learned:

- Any software that commands a satellite is mission critical, even though it may not be embedded in the flight vehicle.
- Validate changes in mission-critical software with more vigor than the original development (Lesson 25, 29, 47). Rigorous formal testing is essential.
- Always specify the units in requirements and Interface specifications.
- Generate expected results used in verification tests independently, in accordance with system requirements.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

80

Check, Double-check, and Triple-check Torquer Phases

The Problem:

A magnetic torquer sign error was caught just one day before launch.

The Cause:

The attitude control engineer who calculated the fields induced by the applied current made an error in an equation, which reversed the predicted torques.

The engineer left the project, and his successor, misunderstanding the vendor's drawing notes, installed all three coils upside down. The second error, which could have been easily discovered with a compass, was masked by the faulty truth table.

Fortunately, the prime contractor's president had concerns with a delay in generating solar power (Lesson 53). As a result, the attitude control components relating to sun acquisition were thoroughly scrutinized.

Two Other Mistakes on This Mission

1. The calculated moments of inertia, which should have been referenced against the center of gravity, were instead referenced against the origin point on the drawing. The mistake was caught by an independent analysis (Lesson 2).
2. The star tracker misbehaved on-orbit because the vendor altered its coordinate convention but the change notice was not heeded.

To alleviate prelaunch work load, the customer paid to bring back the original attitude control engineer. Rechecking his own calculations, he spotted the sign error one day before launch.

Lessons Learned:

- Don't overlook simple tests that can discover problems early.
- Whenever possible, conduct independent analyses.
- Document attitude control coordinate frames early in development to avoid mistakes.

For more technical information, call David Voelkel at (505) 846-8380 or Geoffrey Smit at (310) 336-1602.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

97

Control Hardware and Software Configurations Before, During, and After Tests

The Problem:

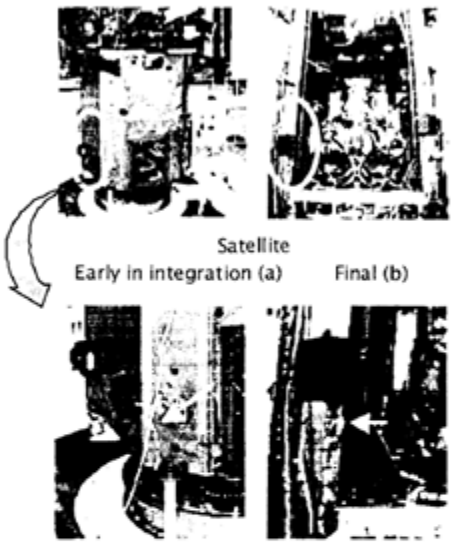
A satellite pointed toward the Sun with the wrong axis.

The Cause:

As the satellite exited eclipse for the first time, it should have pointed a vector 35 degrees off the z-axis toward the Sun. Instead, it wobbled, while pointing the x-axis to the Sun. Fortunately, one of the solar wings was illuminated, giving the engineers time to recover.

The next day, an examination of a photo taken at the launch site revealed that two Sun sensors were mounted ninety degrees off. A software change quickly fixed the problem.

The Sun sensors were mounted on the main access panel in the intended direction during verification testing, before the panel was attached to the spacecraft. When the panel was being installed, however, the mechanical engineers found that the sensor cables were too short to mount the sensors "as hung." Seeing no control document on the sensor configuration, they turned the sensors sideways, without informing the guidance and control (G&C) engineers of the change.



Sun Sensor Misorientation

Lessons Learned:

- Always ascertain G&C actuator phasing (Lessons 53, 60, 80).
- Ensure domain engineers own all aspects of their subsystems.
- Conduct end-to-end testing in the flight configuration.
- Take plenty of photographs during assembly.
- Document G&C subsystem-level alignment. See Guideline GD-ED-2211 from NASA Technical Memorandum 4322A, for example.

For more technical information, call Geoffrey Smit at (310) 336-1602.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Appendix E. Gimbaled vs. Strapdown Inertial Systems

Jerry Gilmore

Draper Laboratory, Cambridge, Massachusetts, July 2006

E-1. Gimbaled IMU Systems

In the Gimbaled IMU System, gyroscopes and accelerometers are mounted on an inner-most gimbal called the "stabilized platform." The gimbal configuration is usually at least a 3-gimbal configuration, though not always with unlimited angular travel along each axis, and operates based on the platform-mounted gyroscope signals in a feedback servo loop through the gimbal torque motors. The gimbaled IMU is usually either operated in the space-stabilization mode, wherein the platform is maintained at an orientation that is nominally fixed (non-rotating) with respect to Inertial Space by nulling the raw sensed gyroscope signals, or else in a commanded platform mode, wherein the gyroscope inertial reference element is suitably commanded so to drive the platform in some prescribed manner (e.g., local-level platform) [refs. 2, 3, 5]. In practice, both forms are commonly used for the same application (e.g., commanded-platform during system calibration and alignment phases, and space-stabilization for subsequent free navigation operational phase). A fourth gimbal is often added to relax flight trajectory constraints otherwise necessary so as to obviate a gimbal lock phenomena that can occur in a 3-gimbal configuration. The gyroscope and accelerometer input axes are typically mounted on the platform so as to provide at least nominally orthogonal triads. The gyroscopes sense platform rotation which, if constantly nulled, as in the space-stabilized mode, implies that the gimbal angle read-out data (which have historically been sine/cosine resolver signals, but could nowadays be optical or other direct angle measure) may be used to determine spacecraft attitude with respect to platform (i.e., for negligible platform drift error, then nominally representing spacecraft attitude with respect to inertial space). And from the spacecraft attitude one may derive the spacecraft inertial rate. In the commanded platform mode, the same principle applies once the commanded platform orientation changes are suitably taken into account.

In the gimbaled IMU space-stabilized mode, the primary error source with regard to platform attitude (i.e., orientation) changes that must be calibrated and compensated is the gyroscope drift (bias) errors and a term identified (and significant for most modern instruments) as gyroscope angle random walk must be kept suitably small. The calibration uncertainty for gyroscope drift is normally quite low, less than 0.01 deg/hr in most deployed IMUs, and the technology is mature. Note that for strict space-stabilized applications, the gyroscopes need not have any appreciable absolute scale factor (SF) read-out accuracy (or compensation thereof) or tight gyro-to-gyro misalignment requirements since any errors thus introduced would be applied to nominally zero platform rate. However, as mentioned above, related pre-flight operations like system calibration and alignment and initialization may introduce other potential gyroscope read-out accuracy considerations driven by the application-dependent character of requisite platform rotation commands.

As mentioned above, spacecraft angular rates, for either space-stabilized or commanded platform mode, are derived from gimbal readout changes. Gimbal torque motors are mounted along the various gimbal rotational axes, and are driven based on nulling the gyroscope signals (i.e., nulling platform disturbances in space-stabilized mode, and nulling disturbances plus

commanded gyroscope reference changes in the commanded platform mode). Thus, the gimbal servo loop response must be capable of following the range of spacecraft dynamics-induced platform disturbances (as coupled through friction and back-emf effects) in order to attenuate them. For crewed spacecraft dynamics, this is not a design obstacle. The 3-gimbal IMU functional representation as used in Apollo is illustrated in Figure E-1.

The HAINS used for the Shuttle implements a 4-gimbal IMU and uses 2-DoF gyroscopes. In space operations, the accelerometers are used to effect guidance closed loop velocity changes. Since the stable platform, via the gyroscope sensing, maintains the accelerometers in a nominally inertial reference frame, a specific delta-v vector change in a closed-loop propulsion burn is achieved by sensing the accelerometer output. In the case of the accelerometers, the primary error sources arise from uncertainty in the bias and scale factor compensation parameters. The scale factor will not be perfectly calibrated and will have some error in the estimated ratio. Typically, this error is characterized as one of two equivalent values, either as a ppm error or as an error percentage. The scale factor can also have nonlinearity errors. The linearity error of the scale factor is also described as a ppm error or as a percentage of the sensor's full scale range.

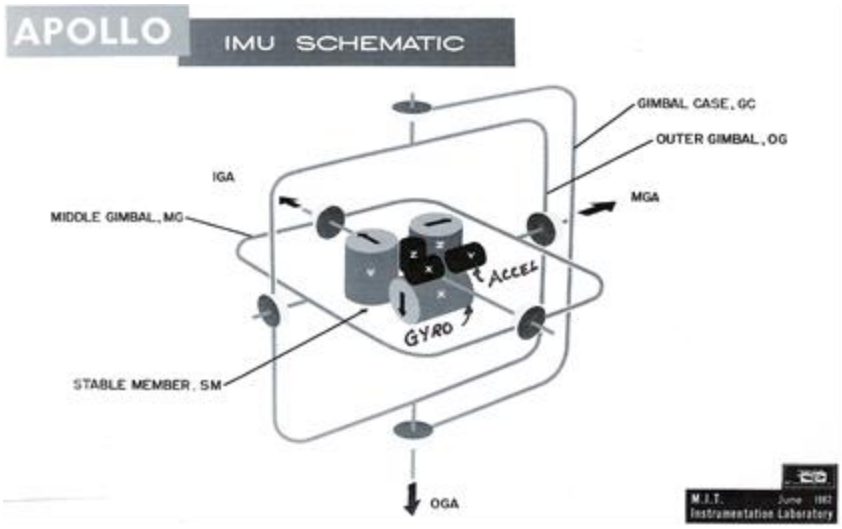


Figure E-1. 3-Gimbal IMU Configuration *(Draper Laboratory, Apollo Photo Repository)*

As alluded to earlier, in prelaunch test of the IMU in the spacecraft with reference velocity and attitude, using gimbal or gyroscope commands (depending on the performance and characteristics of the gyroscopes) to orient the instrument platform with respect to the Earth rate vector and the g vector, a straightforward calibration of the gyroscope and accelerometer errors of interest can be performed [refs. 4, 5]. This method is exercised routinely in Shuttle operations and provides an excellent IMU flight readiness validation method. This capability is useful for applications that have reusable spacecraft missions, such as the Shuttle. Shuttle IMUs have demonstrated a mean time between failure (MTBF) on the order of 5,000 hours across flights.

E-2. Strapdown IMU

Strapdown IMU technology corresponds to the (usually shock isolated) mounting of the gyroscopes and accelerometers on the spacecraft structure via a mounting block. The gyroscopes and accelerometers are mounted within the block to yield a set of nominally orthogonal co-

aligned gyroscope and accelerometer triad input axes. In integrated fault tolerant strapdown configurations, a skewed array of greater than 3 gyroscopes and accelerometers is used. The measurement data provided by the gyroscopes and accelerometers are now in an spacecraft body fixed reference frame (of permissibly high angular rate), and for use in guidance the accelerometer data must be transformed into a suitable navigation frame for velocity and position integration (e.g., often an inertial frame, as henceforth assumed, and as approximately represented by the gyrostabilized platform of the gimbaled IMU). To determine the instrument block attitude and inertial velocity, the body rate gyroscope measurements must be computationally processed, typically using a Direction Cosine or Quaternion (q) integration algorithm, to yield the body-to-inertial attitude representation. Similarly, the accelerometer measurements are transformed into the navigation frame using the computed inertial attitude. Figure E-2 illustrates a typical IMU navigation processing flow, which might be taken for a gimbaled platform or strapdown instrument configuration according to whether the platform or spacecraft body attitude is being computed and used for velocity integration.

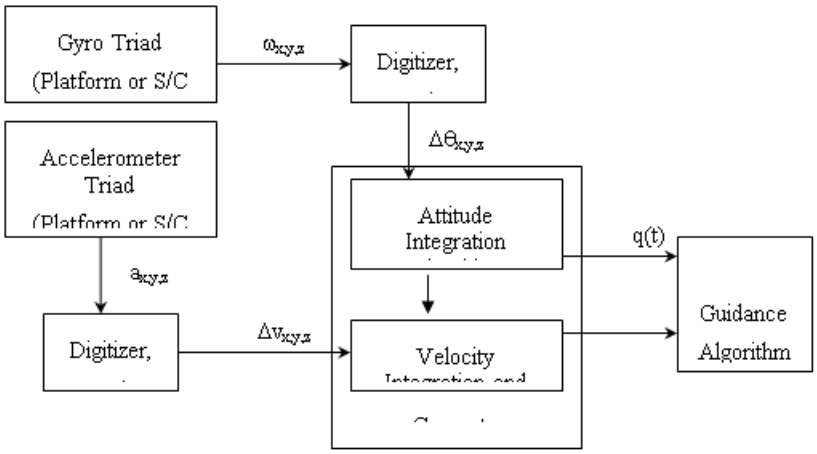


Figure E-2. Navigation Block Diagram

The distinction of the strapdown configuration, then, is that to successfully achieve satisfactory performance, the computational algorithm processing (i.e., attitude integration as well as the implied instrument compensation) must be of high fidelity and with adequately higher speed to accommodate the appreciably more extreme spacecraft angular dynamic environment imposed on the instrument cluster [ref. 1].

Strapdown designs became realizable with the advent of avionic scale digital computer technology. Figure 2 shows both 3-gyroscope and 3-accelerometer triads. In the case of an integrated fail operational (FO) IMU implementation using a skewed gyroscope and accelerometer array, an additional computational transformation is used to generate Triad body rate and acceleration representations.

In the strapdown IMU design, the gyroscope must measure the full range of vehicle dynamic rate angular motion and retain measurement performance—typically to better than 0.01 degrees/hour. For example, assuming a maximum rate of 60 degrees/s, this would correspond to measurement

range of over 106 orders of magnitude. Issues that arise for this dynamic range are obtaining fine resolution $\Delta\theta$ and an accurate stable measurement scale factor in the low ppm range. Since the unit in such an application is subject to the full rate angular motion, constraints arise on the selection of the accelerometer so as to assure that its performance is not degraded by this angular rate (including all vibratory aspects).

As in the case of the gimbaled IMU, a primary gyroscope error source that must be compensated is the gyroscope drift (bias) errors and also knowledge of angle random walk is similarly important for error analysis. However, of especial importance for strapdown IMU is the compensation for the gyroscope readout scale factor, which must also remain stable over time, and often the misalignments as well. However, unlike the gimbaled IMU implementation, a basic strapdown system cannot be accurately calibrated in the spacecraft. Calibration requires removal and test on a test table that enables orientation of the IMU with respect to Earth rate, and g-vector. Additionally, multiple orientations on a rate table are required. This circumstance presents an issue in establishing confident readiness conditions for reusable S/C applications. Additionally, if removals and calibrations are made, the question of stability across power-offs, physical removal, and reinstallation must be verified.

The principal advantage worth noting with regard to a strapdown configuration is that strapdown hardware is generally far less complex than that of the mechanically gimbaled IMU. Also, repair (e.g. replacement of instruments) is considerably less difficult, resulting in lower costs.

E-3. Space Applications of IMUs

As noted above, gimbaled IMUs were designed into both Apollo (3-gimbal) and Shuttle (4-gimbal).

Two integrated inertial-strapdown embedded GPS systems are used on the ISS. GPS is available in LEO, and IMU position and attitude errors can be bounded. Time critical issues with respect to GN&C are not an issue, and angular rate dynamics are essentially benign.

Strapdown IRUs (IRUs do not include accelerometers) are used on orbiting spacecraft, where two units are typically implemented in an operational and standby mechanization. In this application, time criticality is not an issue and spacecraft attitude maneuvers with star tracker measurements can provide an acceptable level of SF calibration and sightings across time intervals, which allows for bounding of drift errors. Nominal maneuver profiles and rates are relatively modest.

A strapdown IMU implementation is used in the Delta launch vehicle. Calibration is performed prior to installation, and sufficient stability is achieved across test and installation. The Delta uses an integrated IMU configuration with six gyroscopes to achieve a robust FO capability. Comparison of gyroscope measurements and automatic fault detection and isolation provides a measure of confidence that ensures a successful launch mission. Techniques have been developed by Draper to permit a measure of self-recalibration in an integrated design of this nature. Note that the Delta is not a reusable vehicle.

Currently integrated strapdown/GPS systems are routinely found in aircraft and missile applications. If antenna locations are appropriate, the GPS (via filtering techniques) bounds inertial error growth and the combined performance provides quality navigation performance.

It is unlikely that GPS operation capabilities are realizable for lunar missions. Additionally, these missions are likely to include multiple rendezvous points, placing requirements on SF performance. In-flight star tracker measurements during transit phase will provide a measure of IMU calibration capability. The issue of implementation and readiness verification of strapdown IMUs for reusable spacecraft operations and extended mission durations remain. Any commitment to an inertial system for future crewed flight missions requires a thorough assessment of calibration stability characteristics, especially in the case of selected strapdown IMUs.

E-4. References

1. "Modern Inertial Technology," 2nd Edition, Anthony Lawrence (Springer, 1998); Ch. 1; Ch. 16.
2. "Avionics Navigation Systems," Edited by Kayton and Fried (Wiley, 1969); Ch. 7.
3. "Aerospace Avionics Systems," George M. Siouris (Academic Press, 1993); Ch. 4, pp. 135-137; 187-188.
4. "Fundamentals of High Accuracy Inertial Navigation," Averil B. Chatfield, (AIAA, 1997); Ch. 1, pp. 5-7; Ch. 5.
5. "Inertial Navigation Systems with Geodetic Applications," Christopher Jekeli, (de Gruyter, 2000); Ch. 4, pp. 101-107; Ch. 8, pp. 238-244.

Appendix F. Apollo GN&C System Components

The following is taken from Draper Lab Report R-700 Volume 1 & Volume III

The goal of the Apollo Project was to place human exploration teams onto the moon and return them safely to earth. A spaceship consisting of three modules was launched on a trajectory to the moon by a Saturn V launch vehicle. The Command Module (CM), designed for atmospheric re-entry, was the home for the three-man crew during most of the trip. The Service Module (SM) provided maneuver propulsion, power, and expendable supplies, and was jettisoned before re-entry into earth atmosphere. The Lunar Module (LM) made the lunar descent. It carried two of the three crew members to the lunar surface while the other two modules remained in lunar orbit. It then returned to lunar orbit, rejoined the CM, and was jettisoned after crew transfer.

The SATURN guidance equipment in the SATURN Instrument Control Unit actually provided GN&C during launch, while the Apollo guidance equipment in the CM provided a monitor of SATURN performance, as well as monitoring by ground-based equipment. Saturn IVB also controlled the Trans lunar injection.

After launch, the Apollo Guidance and Navigation System was the primary onboard equipment that provided guidance and control for all of the midcourse burns, lunar orbit injection, trans-Earth burn, and entry guidance. The Apollo guidance system received position updates from the DSP network, which the on-board system propagated based on the velocity and state vector between updates. The onboard system determined the spacecraft velocity and controlled its attitude maneuvers and velocity burns. The guidance equipment contained in both the CM and the LM were identical except for the optics. The LM had the addition of a Rendezvous and Landing Radar. Both CM and LM carried identical Apollo Guidance Computers (AGCs), which played the central role in the GN&C system operation. The AGC received and transmitted data and commands appropriately from and to the other components and subsystems. Major control functions of the AGC were: alignment of the IMU, processing of radar data, management of astronaut display and controls, and generation of commands for spacecraft engine control. Although technically a “general purpose computer,” the AGC was customized design essentially for GN&C functions operating with a priority driven operating system with a very specialized I/O. The AGC solved the guidance, navigation and control equations required for the lunar mission. The AGC SW in the CSM was programmed for the TLI, the Lunar orbit capture, the Trans Earth trajectory and the entry phases The AGC in the LM carried the SW for Lunar landing, ascent, and rendezvous. With good fortune SW that enabled the LM to drive the CSM (Life Boat) used in Apollo 13 was also resident in the LM computer.

The computer received data and instructions from the ground by radio telemetry and sent back data of interest for mission control. The astronaut with his hand controller could command the computer to execute rotational and translational maneuvers. The IMU, a 3-gimballed design, presented a concern with respect to Gimbal lock possibilities but weight and considerations were paramount. It was configured with 3 single-DoF (SDF) gyroscopes and 3 SDF accelerometers. The IMU provided the measure of spacecraft attitude. The IMU accelerometers measured the linear-acceleration components being experienced. AGC guidance control vector changes (i.e., delta-Vs) determined by the trajectory calculations in the computer were commanded in each of the flight phases. The accelerometers held by the IMU in the inertial frame measured the delta-V

vector and were fed back to the AGC control of the engine gimbals, which shut the engine down. In entry, the IMU and accelerometers measured the aerodynamic trajectory for landing.

Astronauts used the articulating optical subsystems to visually measure direction to stars for IMU alignment. The CM optics included both scanning telescope (wide field of view) and sextant (narrow field of view). Sextant read-out accuracy was 20 arc-seconds—the LM contained only a simple optical periscope, called an AOT.

The LM carried a landing radar on its descent stage. The LM descent stage remained on the Moon. The ascent stage carried a gimbaled tracking radar called the Rendezvous Radar (RR). The RR provided range, range rate velocity and angular direction with respect to the CM during rendezvous, when the LM was returning to the orbiting CM from the lunar surface. The LM was the active member in catching up to, aligning with, and matching the speed of the CM for docking. The CM used the inter-module VHF communication system to measure range as backup. After rendezvous and crew transfer, the LM ascent stage was jettisoned.

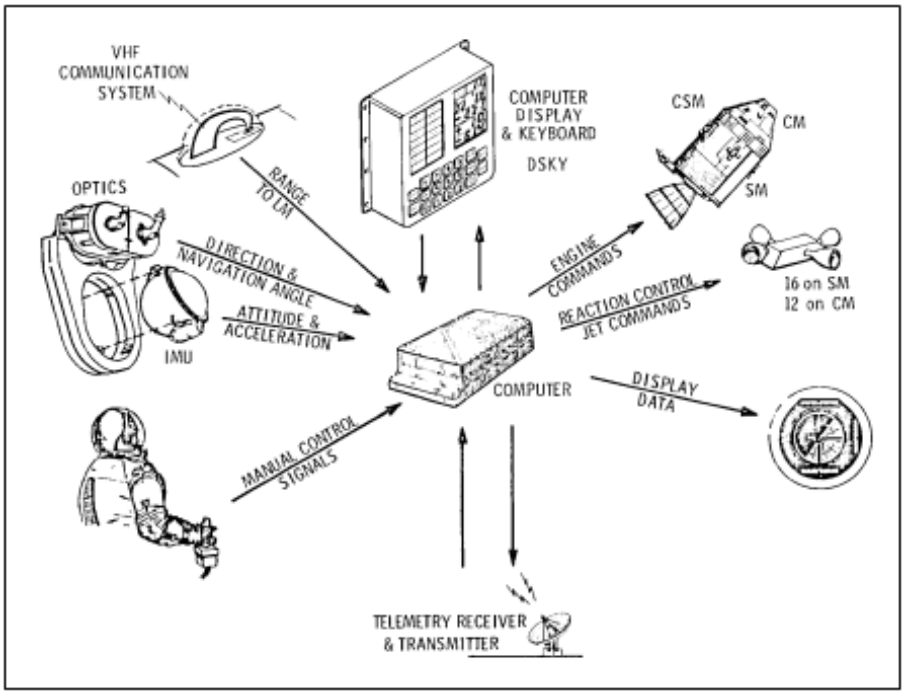


Figure F-1. APOLLO CM GN&C

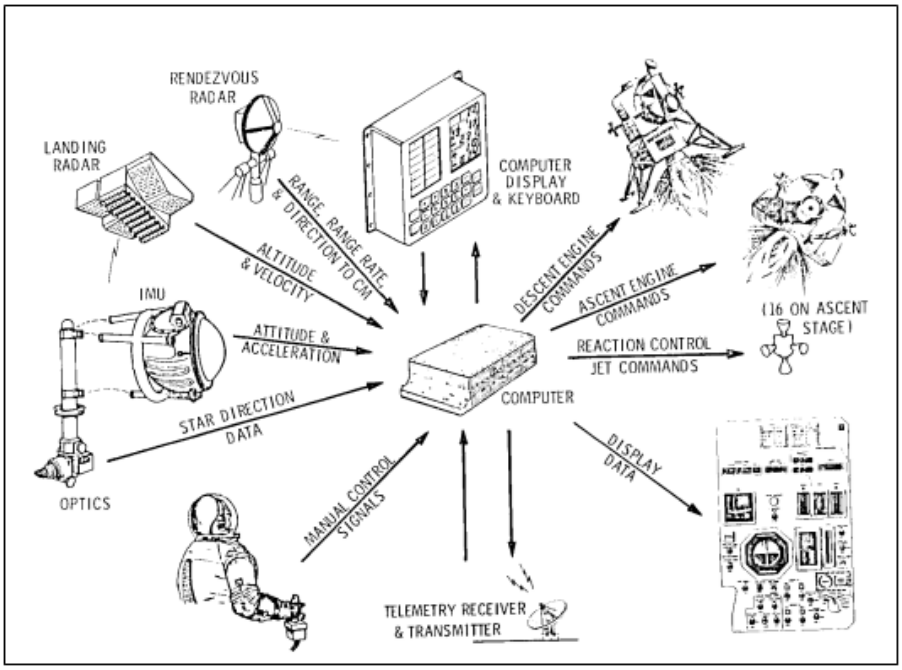


Figure F-2. APOLLO LM GN&C

GN&C equipment not represented in these figures includes key interface and control components: the PSA, the electronics that operated the controls and servos for the IMU and the CSM optics, the CDU that provided all the digital encoded signals from the IMU, the scan telescope and SXT to the computer, and all the analog A/D control data I/O from the computer to the SM thruster, the LM RR, and the Saturn IVB in case of a failure of Saturn (fortunately never used), the PIPA electronics that controlled the accelerometers and digitized its measurements to the computer, the Signal Conditioner Assembly that interfaced to the TLM equipment to provide critical status of G&C system power and temperatures.

F-1. Reliability, Redundancy, Fault Tolerance

Apollo mission success required a full-up functioning and performing GN&C system. Yet the Apollo system was a single string mechanization with no redundant features. Thus, mission success depended on system reliability.

F-2. Reliability

To achieve reliability, rigid control was in place on all parts used, with special NASA fabrication lines using NASA-certified trained assemblers. Special reliability screening methods were in place for the inertial components (e.g., gyroscopes and accelerometers), for example on the order of 230 gyroscopes in a 270 lot build were rejected on the basis of a “failure prediction screening test.” Inspections of the build lines at the industrial contractors were continuously performed.

At the electronic device level, all devices were tested—if a sample in a run proved defective, then the entire lot was quarantined. Failed devices went through detailed teardown failure analysis to preclude defect migration problems. Extensive component-level testing, stress testing, and integrated G&C system testing were performed. A flight readiness certification was made on all systems. Integrated system-level tests were conducted at MIT/IL and NASA JSC.

Astronaut participation in the development cycle and training was typical and intensive. It resulted in several changes that enhanced manual operation and was invaluable in handling contingency problems that arose during flight missions.

F-3. Fault Tolerance

The Apollo computer had the ability to detect faults using built-in test circuits, since it was known that digital equipment was sensitive to transient disturbances and a method of recovery from transient faults was desirable. The outputs of these fault detection circuits generated a computer restart, i.e., transfer of control to a fixed program address. In addition, an indicator display was turned on. If the fault was transient in nature, the restart would succeed and the restart display could be cleared by depressing the Error Reset key. If the fault was a hard failure, the restart display would persist and a switch to a backup mode of operation was indicated.

The failure tolerance in Apollo systems was based on the deliberate design guideline that any single failure should, if at all possible, leave enough working equipment remaining to abort the mission and bring the crew safely home. Although for practical reasons this guideline could not be met everywhere, the number of safety-critical flight items that had no backup was quite small.

The GN&C equipment in particular was designed with enough flexibility in equipment and computer programs to support the measurements and maneuvers necessary for all reasonable mission-abort trajectories caused by failures in other parts of the spacecraft [R-700].

Component	Description	Performance
Computer	AGC (Block II): Priority-interrupt driven, parallel 16-bit, 1-MHz digital computer. 36 K ROM, 2 K RAM 1 ft^3, 70 lb, 55 W 1 each: CM & LM	No failures during missions 19 Failures caught by testing (Integration, Pre-Launch, Vibration, Thermal Cycle) while in "On Flight" status
IMU	A three-degree-of-freedom gimbaled platform isolating three single-degree-of-freedom gyroscopes and three single-axis accelerometers 1 each: CM & LM	No Failures during missions Failures caught by testing in On Flight status
Optical Subsystem	A two-line-of-sight, 28-power, narrow field-of-view sextant and a single-line-of-sight, unity-power, wide field-of-view scanning telescope: CM A unity-power periscope: LM	No Failures during missions Failures caught by testing in On Flight status
Telemetry and Ranging	Rendezvous Radar: LM Landing Radar: LM Telemetry Receiver and Transmitter (to Ground Segment): 1 each CM & LM VHF Communication Used by CM for Ranging to LM	No Failures during missions Failures caught by testing in On Flight status
Pilot Controls	Joystick-type Manual Control Input: CM & LM	No failures during missions Failures caught by testing in On Flight status
Displays	Display & Keyboard (DSKY): 2 in CM, 1 in LM Ball Attitude Indicator, Attitude Error Needles: CM & LM Pilot Control	No Failures during missions 36 Failures caught by testing in On Flight status

The following is a brief bibliography of Apollo-era fault tolerance and reliability analyses:

- Control, Guidance and Navigation for Advanced Manned Missions, R-0600, 1968.
  - Control, Guidance and Navigation for Advanced Manned Missions (R-600, Vol. 2), Final Report on Task II (Multiprocessor Computer subsystem), 1967.
- Alonso, A Multiprocessing Structure, E-2097, 1967.
- Stubbs, "Digital Autopilot for Thrust Vector Control of the Apollo CSM and CSM/LM Vehicles," R-670, 1969.
- Mallach, "Analysis of a Multiprocessor Guidance Computer," Ph.D. thesis, T-515, 1969.
- Hopkins, New Standard for Information Processing Systems for Manned Space Flight, R-646, 1969.
  - This paper discusses the evolution of spaceborne information processing through the

Apollo program to the threshold of the next generation of space vehicles. With the emergence of new manned-space-mission goals, it has become apparent that an integrated system approach to information processing is one of the primary requirements for meeting goals of longevity, economy, and sophistication. The paper outlines a proposed system of computers, multiplexers, dedicated processors, displays, sensors, and effectors configured to execute all checkout, computation, control, communication, and data reduction formerly handled by independent systems on board and on the ground.

- Crisp, SIRU, E-2407, 1969.
- Schwartz, DCA computer, E-2590, 1970.
- Hopkins, "A Fault-Tolerant Information Processing System for Advanced Control, Guidance, and Navigation," R-659, 1970.
  - This report describes continued development of a spaceborne multiprocessor concept reported in MIT/IL Report R-600, Vol. 2. This report discusses system concepts, multiprocessor structure, local processor complexes, and applications to a reaction control system, data bus design, and packaging concepts.
- Hopkins, "Fault-Tolerant Info Processing Concept," R682, 1970.
- Bowler, "Apollo Guidance Computer Improvement Study," E-2463, 1970.
- Laning, "Demand-Actuated Multiplexing," E-2492, 1970.
- Weinstein, "An Efficient Intercommunications Scheme for the Elements of a Real-Time Data Management System," E-2588, 1971.
- Hall, "Reliability History of the AGC," R-713, 1972 (see also R-646, 1969).
- Weinstein, "Software-Implemented Error-Detection and Recovery Techniques for an Avionics Control System," R-781, 1973.
- Smith, "A Highly Modular Fault-Tolerant Computer System," Ph.D. Thesis, T-595, 1973.
- Allen, "Avionic Computer Design Considerations," E-2786, 1973.
- Hopkins, "Computer Control for Manned and Automated Space Vehicles," E-2756, 1973.
- Hopkins, et al, "Evolution of Fault-tolerant Computing at CSDL (1955-1986)," P-2701, 1986.
  - Fault-tolerant computing became an issue of importance at the Draper Lab at the same time digital computers began to be incorporated into GN&C systems. Early systems emphasized fault avoidance, with satisfactory results. More complex systems, which followed, incorporated redundancy. Early redundancy architecture was constrained by size, weight, and cost penalties, and tended toward standby dual forms. As integrated circuits grew in complexity, more massive forms of redundancy evolved in Draper's architectures. The challenge of full-time, full-authority control of commercial aircraft motivated a number of research activities directed toward the realization of extremely low system failure rates. These activities revealed substantial problems to be encountered in the practical realization of redundant systems, even though such systems seem extremely simple in abstraction. One example of such problems is the synchronization of redundant clocks, where a fundamental rule was discovered that later emerged in a more general form as the "Byzantine generals problem." A hybrid-redundant multiprocessor with reconfigurable triad (FTMP) resulted from the research. More recent research capitalized on large-scale integrated circuits, as well as fault-tolerant system architectures of the past, to yield a modular n-redundant, tightly synchronized computer, virtually

transparent to software, thus able to capture software written for simplex systems, including certain n-version software forms. Computers of this type are being deployed in numerous applications.

Appendix G. Use of Bond Number to Determine Liquid Slosh Regime

From "Persistent Challenges in Aerospace Dynamics and Control Verification and Validation" presentation, Jeb S. Orr, September 1, 2022

Dynamic fluid phenomena can be broadly classified by Bond and Weber number:

$$Bo = \frac{\rho \bar{g} a^2}{\sigma} \qquad We = \frac{\rho v^2 a}{\sigma}$$

- Bond number is used to describe the transition into gravity-dominated flows (high-G slosh).
- Weber number is used to describe the transition into capillary-dominated flows (i.e., PMDs).

The parameters are:

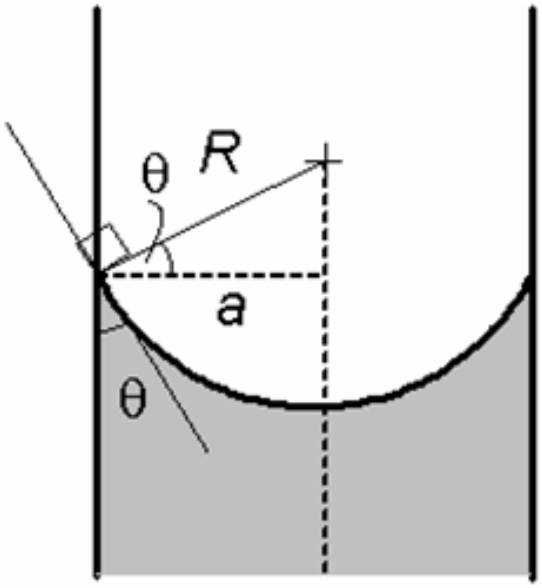
- Mean or quasi-steady axial acceleration $\bar{g}$
- Characteristic length or cylinder radius *a* and velocity *v*
- Fluid density ρ, surface tension σ.
- A critical parameter for the capillary regime is the contact angle, which depends on surface tension, materials, and temperature.

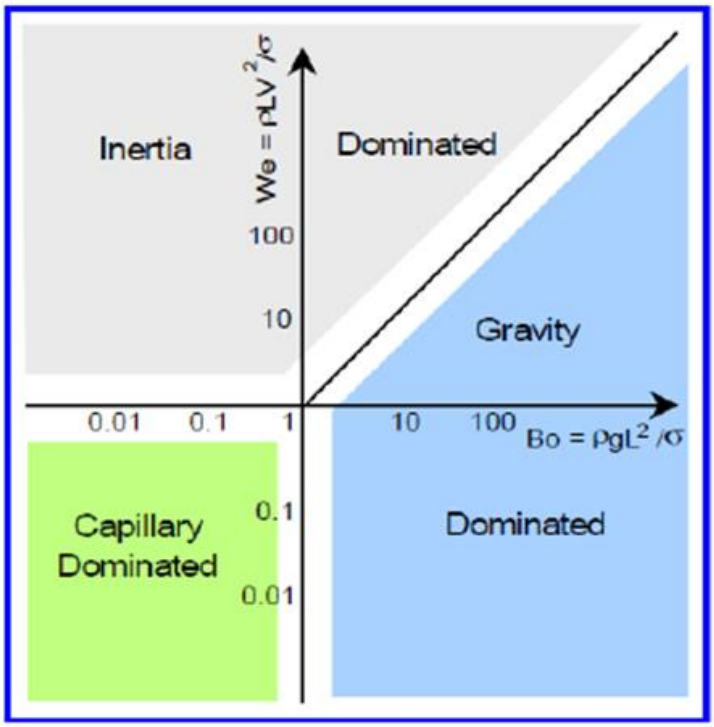
High-G slosh regime (Bo > 1000)

Low-G slosh regime (~30 < Bo < 1000)

Microgravity slosh regime (Bo < ~30)

[From Dodge, ref. 40]





[From Dodge, ref. 40]

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/17/2023	Technical Publication	

4. TITLE AND SUBTITLE
Best Practices for the Design, Development, and Operation of Robust and Reliable Space Vehicle Guidance, Navigation, and Control Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dennehy, Cornelius J.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
869021.01.23.01.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
NESC-RP-22-01762

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TP-20230005922

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category Space Transportation and Safety
Availability: NASA STI Program (757) 864-9658

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This document summarizes and updates the NASA Engineering and Safety Center Guidance, Navigation, and Control (GN&C) Technical Discipline Team's (TDT) work to synthesize and document the current best practices for the design & development of robust and reliable GN&C systems for robotic and crewed (human-rated) spacecraft. These GN&C best practices for future science and exploration missions were derived from the lessons learned, both positive and negative, on earlier spaceflight projects, both robotic and crewed. An attempt has been made to capture preferred practices that reflect the key considerations, trades, and processes directly attributed to past mission success.

15. SUBJECT TERMS
Guidance, Navigation, and Control; NASA Engineering and Safety Center; Best Practices

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	297	(443) 757-5802