SPACECRAFT COMPUTER SYSTEM DESIGN CONSIDERATIONS FOR A PILOTED MISSION TO MARS

Edward N. Brown

INTRODUCTION

Piloted deep space missions, such as a human mission to Mars, present new challenges in the design of spacecraft computer systems. Because of the human element involved, the demands of the operational mission, and the constraints imposed by weight, electrical power, reliability, environmental (especially radiation), and data processing performance considerations, general-purpose consumer or business oriented computer solutions are not acceptable [1]. That does not imply that every circuit and every microchip for the computer system needs to be designed and constructed from scratch. Some may indeed be, but most will be developed by utilizing, modifying, or tweaking existing designs and products. But it's not as simple as just selecting top-rated top-value components from a computer catalog or store shelf, hooking them up, and then fine-tuning the result. That system won't do the job. The solution for this application must be engineered. What this really means is that it is not sufficient to simply state that the system must be "user-friendly, long life, low weight, low power, high reliability, robust quality, and high performance". Like many other complex designs, "the devil is in the details" [2] and that is especially true in this application. While these design characteristics are valid, exactly how best to achieve them is a very difficult task. There are many questions to answer. How reliable does it need to be? How much power should it consume? How small does it need to be? How much processing throughput should it have? These are just some of the major and more obvious questions. A myriad of questions will present themselves as each area is investigated. The engineering challenge is to determine the optimal or appropriate levels and tradeoffs (quantitative where possible) among these characteristics such that all the operational, system design, and programmatic requirements (cost and schedule being just another two parametric constraints) are satisfied and the system contribution to overall mission success can be assured to a level that is acceptable to all the stakeholders. The best way to systematically go about doing this is to utilize standard Systems Engineering procedures and techniques to flush out the driving design requirements and eventually synthesize a working design [3]. This approach is described in the paper.

APPROACH

To determine the design drivers for a system definition, four different perspectives can be combined in an analytical framework. First, we must look backward to the experience gained and lessons learned from earlier human spaceflight endeavors, such as Apollo, Skylab, Space Shuttle, and International Space Station (ISS) [although Space Stations have a different design perspective because they are more akin to habitats than to transportation vehicles] as well as from unmanned deep space missions. This can provide valuable insight into the best way to move forward by not making the same mistakes that were previously made over again, and by keeping certain design approaches that previously were found to be successful as precepts. Second, we must understand the vision, goals, objectives, and operational concepts of reputable entities associated with Mars exploration, such as the Mars Direct Mission, NASA Mars Reference Mission, or ISTC Project 1172. This is required since the design must be tailored to fit the mission and not be a general-purpose or one-size-fits-all type of design. Thirdly, we must understand the current commercial technological state-of-the-art by examining the computer products of industry leaders in both the manufacturing (hardware and software) and system integration areas (especially in the telecommunications industry). This will likely strongly affect the actual design synthesis because it is usually more expeditious to utilize or adapt an existing design than to initiate a design from scratch. Finally, we must review active computer technology R&D programs currently being pursued by government, university, and industrial R&D Labs that have applications to spacecraft design, in order to ascertain the directions, thrust, and focus of these endeavors. This will insure that our design perspective is not “out-of-kilter” with other efforts and that we have a project level information and technology base in which to leverage off.

Therefore, the process can be simplified to the answering of four questions:

1) What are the design requirement drivers based on the raison d’etre and ‘lessons-learned’ from both past and present human spaceflight and robotic spaceflight program designs?
2) What are the design requirement drivers as dictated by the most generally accepted mission concept?
3) What are the design requirement drivers that result from an understanding of today’s commercial state-of-the-art industrial computer product technology and projected future trends?
4) What are the design requirement drivers resulting from analyses of active ongoing R&D programs concerned with computer technology development applicable to space vehicle design?

In the process of investigating questions 1, 3, and 4 above, certain guiding principles of system design will emerge. These principles may be driven by performance, cost, or programmatic concerns, but they will represent the technological bounds within which the system will have to be designed.

PERSPECTIVE

In human spaceflight projects to date, custom designs, military designs, and carefully modified commercial designs have predominated. However, since 1994 the DOD has led an effort to utilize open system architectures and ruggedized industrial grade commercial off-the-shelf components to the greatest extent possible in the design of vehicular and shipborne computing platforms [4]. NASA JPL has embraced this philosophy in concert with robotic space projects developed under the “faster, better, cheaper” mantra [5]. Although there has been mixed success in the application of COTS/Open Systems to date, this has now become a mature guiding principle of system design that is meant to counter the high expense, long lifetime inalterability, and undesired supplier dependencies associated with earlier custom Mil-Spec system designs [6]. Observance of this principle will allow future DOD and NASA programs to leverage off rapid growth of computer and information technologies now occurring in the commercial marketplace. There is no reason to believe that this overarching precept will not also be applicable to the design of the fleet of spacecraft that will carry humans to Mars (although some specific exclusions are probably inevitable). The benefits and payoffs of using COTS/Open Systems are just too great to ignore and it has become the modus operandi for implementing all but the most critical or the most sensitive functional requirements.

In addition, certain design integration approaches that have evolved over the past decade, such as distributed, integrated, modular, and miniaturized avionics [7], will be the cornerstones upon which the computer design of the Mars vehicle will be based. Fundamental design concepts, such as the de-centralization of functionality, the utility of embedded computer control of almost all spacecraft systems, the need for reliable and timely communications between all computing elements, and the ability to detect, isolate, and reconfigure around faulty elements, will dictate that certain design directions be followed. An example of such a direction is the use of network-centric system topologies with protocol driven information transactions instead of unique point-to-point user defined data transactions. This broad understanding of design directions will provide the high level guidelines from which the more detailed drivers to the final spacecraft computer system design will emerge.

Therefore, it is necessary to add a fifth question to the above four in order to complete the overall investigative arena.

5) How do the answers to the above four questions synthesize together with the high level guidelines that have evolved from the COTS/Open Systems paradigm and distributed/integrated/modular/miniaturized avionics concepts?

When answers to these five questions begin to materialize, we will start to accumulate a knowledge base of information regarding the desired attributes of the computer and data processing systems that would likely be onboard a piloted spacecraft on a mission to Mars. As the knowledge base matures, a set of preliminary system design requirements (including identified design drivers) will eventually be derived and formulated in appropriate specification type language. From these high-level system requirements, a preliminary architecture and notional system design, with performance metrics, will eventually emerge.

MANNED VS. UNMANNED SPACECRAFT

However, prior to delving into the analyses proper, it is necessary to understand and appreciate the key differences and similarities between manned and unmanned spacecraft, and in particular, between computer systems designed for manned spacecraft and computer systems designed for unmanned spacecraft. Although a human mission to Mars will obviously utilize a manned spacecraft, the operational mission design and logistics will be similar to that which has already driven the design of deep space unmanned robotic spacecraft. So there is a synergism that can be obtained by examining the attributes of each (Note that unmanned earth orbiting satellites are intentionally omitted from this comparison although powerful computer systems onboard large communication satellites are worthy of review and should be evaluated in connection with the analysis involved in answering questions 3 and 4).

Spacecraft computers designed for both manned and unmanned missions share a number of key attributes:

- May need to operate over long mission times
- Need to minimize power, weight, size requirements
- Need for autonomous operation under certain conditions
- Need for robust fault tolerance and reliability
- Need for automatic FDIR (fault detection, isolation, recovery)
- Need for efficient and reliable telemetry
- Need for robust environmental qualification
- Need for resource management
- Need for high computational and processing performance

Both designs must accommodate these concerns although the degree of concern and the level of specification is really determined on a case-by-case basis and is often driven by the greater vehicle design that provides the platform for the computer system or by the mission requirements. For example, because of the small physical size of unmanned probes, the need to minimize power, weight, and size is extremely important and is usually a fundamental driving requirement, whereas for manned spacecraft it may be a goal or negotiable requirement. The actual specified values in each case will be driven by the vehicle design constraints. Similarly, the need for autonomous operation and automatic FDIR is very important for unmanned probes because it is driven by mission requirements (e.g. long time out of communications, latency of command signal) but may be equally important for manned spacecraft because of different mission requirements (e.g. crew sleep cycle, small time window hazardous mission phases).

However, because of these differences in spacecraft vehicle design and in mission requirements, there are some fundamental differences in the associated computer system designs that have been installed and operated to date. Table 1 presents a comparison of vehicle and mission characteristics between manned and unmanned spacecraft related to computer system design and operation. A computer system designed for a manned vehicle will likely differ from a computer system designed for an unmanned vehicle because of the differences shown in this Table. It can be seen that some characteristics are unique to the manned system, some characteristics differ in relative value only (due to the vehicle design), and some characteristics differ because of mission requirements or perspective. The top five items form the crux of the comparison. The bottom line is that the primary objective of the computer system on a manned spacecraft is to operate the vehicle, including all the associated subsystems, and service the occupants in a safe and efficient manner, whereas the primary objective of the computer system on an unmanned spacecraft is to operate the vehicle and the sensor instruments in order to obtain the science data and transmit it back to earth. As can be seen from the Table, the presence of a human on the vehicle drives the design direction.

Computer related attributes that are unique to manned spaceflight can be summarized by the following:

- Overarching requirement for Human Safety

  - Safety Driven Design & Development Process
  - Safety Driven Design Architecture
  - Importance of FDIR to operational safety
- Need for User Friendly Human Interface for Situational Awareness
  - Visual Display outputs
  - Tactile Keyboard, Edgekey, and Switch inputs
  - Voice Recognition input
  - Auditory Alarm outputs
- Greater allowable power, size, and weight constraints due to greater available resources driven by human needs
- High throughput and logical processing requirements to accommodate real time automatic control and monitoring of spacecraft systems and to accommodate flight crew needs for manual monitoring and commanding of spacecraft systems
- Allowance for onboard in-flight maintenance and repair
- Incorporates capability for manual pilot-in-the-loop control of certain flight maneuver and control functions (rendezvous, docking, landing)

Historically, when these attributes were considered during the development process, the resulting design usually contained certain characteristics that differentiated it from a computer system design for an unmanned robotic probe, such as:

- Greater throughput and processing power requirements
- Greater memory requirements
- Greater I/O requirements
- A greater number of larger and more complex programs
  - generally utilizes an Operating System and System Services software
  - more diverse application programs
- A sophisticated human interface
- More complex Redundancy Management and synchronization requirements
- Incorporated Central Processing Units (CPUs) and Microprocessors (uPs) instead of Digital Signal Processors (DSPs) and Microcontrollers (uCs)
- Greater power dissipation and cooling needs
- Greater concern for radiation induced Single Event Upsets (SEUs) and Single Event Effects (SEEs)
- Larger footprint
  and
- Longer development time and higher cost

In fact, because of these demanding requirements, multiple computers or processors were often used for different functions. For example, the flight control computer, the command & control computer, the systems management computer, the display driver computer, the engine control computer, and the I/O computer may all utilize separate processors and be located on separate cards or even in separate Line Replaceable Units (LRUs). Mass memory, timing controllers, and backup systems may also be in separate cards or boxes. That is not to say that future manned spacecraft computer designs will follow this tendency. That's just how it happens to be today. Although the attributes, characteristics, and requirements will be similar, the actual design implementation will change according to the high level guidelines and directions that are in effect at the time.

The key to the design of the computer system for the manned Mars mission will be to determine what combination of characteristics and attributes, conventionally associated with either manned or unmanned spacecraft computer systems, represents the best characteristics and attributes for the manned Mars mission.

SUMMARY

The analysis required to answer each of the five questions presented herein is non-trivial and will require careful research and investigation into areas normally affiliated with both manned and unmanned spacecraft design. But this will assure that only the best and most applicable aspects of commercial computer product technology and space vehicle related computer technology R&D will be properly integrated with mission requirements and experiential 'lessons-learned' type knowledge, in order to valuably contribute to the overall design of the spacecraft computer system for the human mission to Mars.

ACKNOWLEDGEMENT

The author is employed as a Principal Engineer/Scientist by The Boeing Company, NASA Systems division, in Huntington Beach, California. However, neither the presentation material, nor the research and preparation work supporting it, was financed by The Boeing Company and therefore does not represent any endorsement or acknowledgement by The Boeing Company. The content herein solely represents the independent analysis and conclusions of the author.

REFERENCES

[1] Tomayko, James E., 1988, *Computers in Spaceflight – The NASA Experience*, NASA Contractor Report 182505,
http://www.hq.nasa.gov/office/pao/History/computers/Compspace.html

[2] A common quotation often applied to computer programming and design meaning that if you do not pay enough attention to the details, you can get burned. See Martin, W. Mike, 1999, *The Devil is in the Details – The Difference Between Programmatic Concepts and Design Concepts*, Lecture, http://bucharest.stanford.edu/KitTemp/1999/Lecture-2-12-99/MikeMartin/Sld001.htm

[3] Schoening, William W., 2000, *Exploring Concepts during Pre-System Definition*, Proceedings of INCOSE 2000, Paper ID 30, Minneapolis

[4] Morgan, Rick, Mark Pacelle, 2001, *Designing Deployed Systems with COTS*, SKY Computers White Paper, http://www.skycomputers.com

[5] Katz, D. S., P. L. Springer, R. Granat, M. Turmon, 1999, *Applications Development for a Parallel COTS Spaceborne Computer*, Third Annual Workshop on High-Performance Embedded Computing, Lexington, Massachusetts, http://pat.jpl.nasa.gov/public/dsk/papers/hpec99.pdf

[6] Foreman, John, 1998, *On the Front Lines of COTS – Lessons Learned, Speculation for the Future*, Tutorial, Software Engineering Institute, Carnegie Mellon University, http://www.stc-online.org/cd-rom/1998/slides/tut2jforeman.pdf

[7] Conmy, Philippa, John McDermid, 2001, *High Level Failure Analysis for Integrated Modular Avionics*, 6th Australian Workshop on Safety Critical Systems and Software, Brisbane, www.jrpit.flinders.edu.au/confpapers/CRPITV3Conmy.pdf

Table 1 Comparison of Spacecraft Computer System Characteristics

Manned	**Unmanned**
Vehicle centric functionality	Payload centric functionality
High logical processing requirements needed for vehicle and crew applications	High computational processing requirements needed for sensor and instrument data
Safety directed design – destination driven	Performance directed design – science driven
Need for onboard user interface for command and display	N/A
Need for accessibility and maintainability	N/A
Importance of auto and manual FDIR (including manually switched backup)	Importance of auto FD and correction
Onboard power generators necessary for life support and thermal control allow for higher power consumption	Low onboard power generators dictate need for low power consumption
Optional reversion to manual operation when comm to MCC is unavailable	Need for autonomous operation when comm to MCC is unavailable
Need to work over short and long missions	Need to work over longer mission times
Greater memory and I/O requirements	Lesser memory and I/O requirements
Basic reliance on tried-and-true technology	More tendency toward innovation and less mature technology