NASA CR-188277

Future Manned Systems Advanced Avionics Study

Advanced Avionics
Johnson Space Center

Final Report

January 1992

Prepared for:
NASA Johnson Space Center
Houston, Texas

Systems and Research Center
3660 Technology Drive
Minneapolis, Minnesota 55418

Future Manned Systems Advanced Avionics Study

Final Report

Prepared for:

NASA Johnson Space Center
Houston, Texas

Prepared by:

Bob Sawamura
Kathie Radke

Honeywell Inc.
Systems and Research Center
3660 Technology Drive
Minneapolis, Minnesota 55418

January 1992

Table of Contents

Table of Contents (Continued)

Section — Page

Table of Contents (Continued)

Section

Page

Table of Contents (Continued)

Section Page

Table of Contents (Concluded)

Section — Page

List of Figures

List of Figures (Concluded)

List of Tables

Executive Summary

S.1 General

COTS+ was defined in this study as commercial off-the-shelf (COTS) products, ruggedized and militarized components, and COTS technology. This study cites the benefits of integrating COTS+ in space, postulates a COTS+ integration methodology, and develops requirements and an architecture to achieve integration. Developmental needs and concerns were identified throughout the study; these needs, concerns, and recommendations relative to their abatement are subsequently presented for further action and study.

The study described a total COTS+ system concept consisting of COTS+ hardware, software, systems, architecture, and their requirements. The Airlines Electronic Engineering Committee (AEEC) draft of Project Paper 651, "Design Guidance for Integrated Modular Avionics," and the Boeing 777 airplane avionics architecture were used extensively to establish the concept.

The concept was implanted from the bottom up into conceptual space avionic architectures representing different future manned mission vehicles. The bottom-up integrations met with future manned mission top-down requirements that were also developed in the study. The melding of integrations with requirements disclosed compatible unions or, in most cases, compatibility differences. These differences were resolved by changes to mission/vehicle requirements, architecture, and/or COTS+ product/testing requirements. Differences requiring further development were identified as needs. Difficult differences were considered concerns. Differences requiring significant involvement, time lapse, or risk were identified as technology gaps.

The COTS+ concept appears attractive. The study baselined a feasible space vehicle architectural approach supported by unique requirements for COTS+ missions, operations, vehicles, and components. The subject of COTS+ in space should not be accepted, de-emphasized, or dismissed by this study; there is much work to be done to further its cause, test its utility, and/or disprove its merits. Detailed work is required to accommodate needs and resolve concerns. In particular, system tradeoff studies must examine the impact of incorporating COTS+ as presented herein. That is, we have taken the approach of minimizing nonrecurring development by using COTS+ in operational environments compatible with COTS+ component design. Our study concludes that future manned space avionic systems may be implemented with such an approach. Nevertheless, a system-level assessment is needed to validate the approach.

S.2 COTS+ Benefits

S.2.1 Reducing Technology Gaps

This study was initiated with a desire to assess integrating COTS+ technology within space avionics to the advantage of the space program. Of the many COTS+ benefits described in the study (cost, capability, dependability, procurement lead times), the effect of shortening procurement lead times with COTS+ technology is significant.

Because COTS+ technology represents present- or near-term technology, its use minimizes space avionics technology gaps. This fact is substantiated by comparing COTS+ product maturities to identified technology gaps. The recent General Dynamics Space Avionics Requirements Study [SPAC90] identifies future manned mission technology gaps that currently exist. The study identified and evaluated 143 critical technologies applicable to space avionic architectures. Technologies were classified into three categories:

- Green—present or near term technology that can be used in a production system within five years.
- Yellow—developmental technology that does not require a major breakthrough.
- Red—a technology gap area that requires a major breakthrough.

By comparing the list of categorized technologies within the Space Avionics Requirements Study to a conservative assessment incorporating COTS+ technology, technology-gap reduction is realized (see Table S-1). Therefore, a benefit of COTS+ technology insertion is the compression of future manned mission timelines providing an economical solution to "space race" scenarios.

Table S-1. Technology Gap Comparison

Class	GDSS Study	With COTS+
Green	29	95
Yellow	101	41
Red	13	7

S.2.2 COTS+ Product Advantages

Several COTS+ products and technologies were described within this study. Their benefits: state-of-the-art performance, maturity, dependability, and low acquisition cost, made them appropriate candidates for inclusion within COTS+ space avionic architectures. Aeronautical Radio, Inc. (ARINC), Boeing 777 aircraft, and Honeywell avionic technologies were found to enhance future manned mission architectures, were described in detail, and were incorporated within strawman architectural configurations. The technologies described in this study are representative of COTS+ technologies available from other vendors; they are:

- Boeing 777Airplane Information Management System (AIMS),
- Boeing 777 AIMS central maintenance computer,
- Honeywell's Boeing 777 flat-panel display system,
- Boeing 777 ARINC 629 bus,
- Boeing 777 ARINC 429 bus,
- Boeing 777 ARINC Fiber Distributed Data Interface (FDDI) network,
- Honeywell's Boeing 777 SAFEbus™* backplane bus,
- Honeywell optical disk storage system,
- Honeywell integrated Inertial Navigation System/Global Positioning System (INS/GPS).

S.3 Requirements

A baseline COTS+ system architecture incorporating commercial aircraft avionic Integrated Modular Avionics (IMA) concepts (a system approach to avionic engineering which takes into account modern thought on system decomposition, modularity, function availability, and fault tolerance) was established. Strawman architectures incorporating the COTS+ concepts with COTS+ products were defined for launch, transfer, orbital/surface, and excursion vehicles. The architecture utilized ARINC 629, 429, and FDDI networks to connect IMA cabinet enclosures, remote data interfaces, and sensors/effectors/displays. COTS+ avionic requirements were generated from the point-of-departure strawman configurations.

Top-down COTS+ avionic requirements from COTS+ reference vehicles and missions were used to modify the avionic requirements. The following statements relate to unique COTS+ requirements generated within this study.

- COTS+ avionics shall be distributed, physically partitioned, and located in environments within their environmental envelopes.
- COTS+ avionics shall be qualified to new acceleration, humidity, and salt spray tests.
- Requirements shall ensure single-event upset (SEU) recovery with error detection and correction (EDAC) mechanisms as well as protection against latchup caused by radiation environments.
- The COTS+ program shall provide for assessment of COTS+ radiation tolerance and possible substitution of more radiation-tolerant parts at the vendor's facility without significant additional recurring cost.
- Acoustic qualification should be required for COTS+ equipment installed in high-acoustic environments such as near engines.
- For extended duration missions, a storm cell, or equivalent will be provided to protect critical avionics from major upsets. A safe will be used for storing COTS+ avionics cold spares.
- COTS+ avionics will be qualified by analysis to ensure that there are no detrimental outgassing effects.
- Any COTS+ equipment that may be operating during the ascent phase in a partial vacuum shall be proved by being operated during the evacuation phase of thermal vacuum chamber testing.
- Configuration control procedures shall be capable of identifying hardware and software configurations that are compatible and constitute a validated configuration. It may be necessary for the equipment design to incorporate safeguards to enforce compatibility.
- The COTS+ parts list applicable to a particular series of vehicles' lists shall identify acceptable alternative parts. This list may include interchangeable components specified by an ARINC characteristic supplied by different manufacturers.
- Remote Data Interface (RDI) avionics without adequate environmental protection shall require environmentally hardened COTS+ components.

SAFEbus™ is a registered trademark of Honeywell Inc.

S.4 Needs and Concerns

Numerous COTS+ needs were noted in the study; most, however, correspond to needs that are also necessary to integrate space qualified parts and technologies. Needs unique to COTS+ integration are cited above in Subsection S.3, Requirements.

One concern was identified: assessment of COTS+ radiation tolerance for transfer, excursion, orbital/surface missions (missions other than earth to orbit). Further study of vehicle sheltering concepts and COTS+ part replacement or other strategies (i.e., spot shielding) is recommended.

S.5 Conclusions and Recommendations

The Future Manned Systems Advanced Avionics Study provided an exploratory investigation of integrating COTS+ products and technologies in space avionic architectures. A comprehensive COTS+ avionic architecture (software, hardware, and system engineering) for space applications was established. The architecture employed COTS+ technology, quad-redundant channels, deferred maintenance (including fly-without-repair), and cold spares concepts. Physically distributed architecture is used to provide avionic environment within COTS+ product environmental envelopes.

The COTS+ concept appears workable in part or in totality. No COTS+ technology gaps were identified; however, radiation tolerance was cited as a concern, and the deferred maintenance issue resurfaced. Further study is recommended to explore COTS+ cost-effectiveness, maintenance philosophy, needs, concerns, and utility metrics. The generation of a development plan to further investigate and integrate COTS+ technology is recommended. A COTS+ transitional integration program is recommended. Sponsoring and establishing technology maturation programs and COTS+ engineering and standards committees are deemed necessary and are recommended for furthering COTS+ integration in space.

Section 1
Introduction

1.1 Scope

This report documents the study we conducted to incorporate commercial off-the-shelf (COTS), ruggedized, and militarized equipment into space vehicles used for future manned mission applications. The study included developing a design philosophy, general requirements, system configurations, recommended procedures and practices, and new maintenance operations. It also identified technologies and further development necessary to use COTS+ products (COTS, ruggedized and militarized components, and COTS technology) for space launch, transfer, orbital, and excursion mission segments.

This study identifies top-level issues, concerns, and problems associated with COTS+ insertions in space applications. To facilitate this identification, a strawman architecture incorporating COTS+ technology and components was developed for future manned missions. Because COTS+ is not readily adaptable to space applications, the differences between the COTS+ components and space-qualified components are noted to identify what changes must be made to incorporate COTS+ technology with minimum impact.

To accommodate the use of COTS+ in space, changes in program philosophy and vehicle/system requirements, including architectural partitioning, are assessed, as well as easily made modifications to COTS+ components. Preliminary vehicle system requirements, COTS+ subsystem requirements, and architectural definitions necessary to implement the COTS+ philosophy are subsequently generated.

This report identifies technology shortfalls and needs, provides development direction, and recommends plans leading toward timely use of COTS+ technology in space.

1.2 Purpose

This report is presented as a top-level application design guide for COTS+ avionics. It provides guidance for the design and implementation of COTS+ avionics for space, which may replace or be used with existing equipment in old designs (backward integration) or for new designs in vehicles designed after 1991. It represents concepts provided by airline representatives, airframe manufacturers, and avionics equipment designers for commercial aircraft avionics as well as the views of the authors.

This report is conceptual in nature and covers broad subjects of operational objectives, fault tolerance, hardware components, software design, and certification issues. In covering all these issues, the document attempts to be as inclusive as possible while being general enough to be applicable to new and developing technologies. It includes design philosophy and recommended practices concerning the use of COTS+ and, as such, is expected to establish a starting point for the actual implementation of COTS+.

1.3 COTS+ Definition

Included within the definition of COTS+ products herein are nondevelopmental items (NDI) covered under Civil Market COTS, Commercial Type, Olive Drab Commercial, Best Commercial Practice, and MIL-SPEC products [USAF22] (see Table 1-1 and Figure 1-1). These NDI classifications pertain to non-space-qualified components that require similar requirements, architecture, and component modifications to be qualified for use in space. Because of the general similarity in their qualification for use in space, all are considered within the scope of this COTS+ study.

Of the above NDI classifications, only Civil Market COTS items fit the formal definition of commercial off-the-shelf. In the strictest sense, all other NDIs cannot be considered commercial off-the-shelf. Civil Market COTS items represent a limited category of commercial products for commercial use. They are bought exactly as found in the civilian market and are allowed to flow with the changes and updates the vendor provides to customers.

The COTS+ product definition also includes government-sponsored Best Commercial Practice hardware designs that, when compared with MIL-SPEC designs, are less rugged and/or are less standardized developments. The contractor is allowed to build a new or modified design that will not stand up to military or space environments but is solid enough to withstand civilian uses. Because they represent a government-sponsored new design, the economics of the high-volume civilian market, lead-time advantages, and up-front development cost savings do not provide significant advantages compared with Civil Market COTS items. Best Commercial Practice hardware is included within this COTS+ study because it covers Civil Market COTS items that must be functionally modified to meet COTS+ architecture requirements. An example of such a modification would be the addition of on-line monitoring or self-test capabilities to an avionic module.

Table 1-1. The Commercial Spectrum

	MIL-SPEC	Best Commercial Practice	Olive Drab Commercial	Commercial-Type ("Special")	COTS
Design Features	Government: Militarized	Government: Not militarized	Commercial: Just for government	COTS: Modified for government	For civil market
Examples	Fighter aircraft	Fixed ground radio	Tactical radio	Embedded computer	Television monitor
Percent of Sales to Government	100%	100%	Probably 100%	Small (of basic item)	Small
Design Disclosure	Full (piece part)	Full (piece part)	Mostly F3* Maybe Full	Probably F3* Full needed	F3*
Configuration Authority	Government	Government	Vendor or foreign government	Domestic or O/S vendor	Domestic or O/S vendor
Design Stability Risk	Low	Low	Moderate to low	Moderate to high	High
Long-Term Support/ Cost Risk	Low	Low	Moderate	High	Moderate to high

C910899-39A

*Form, fit and function

Reference [USAF 22]

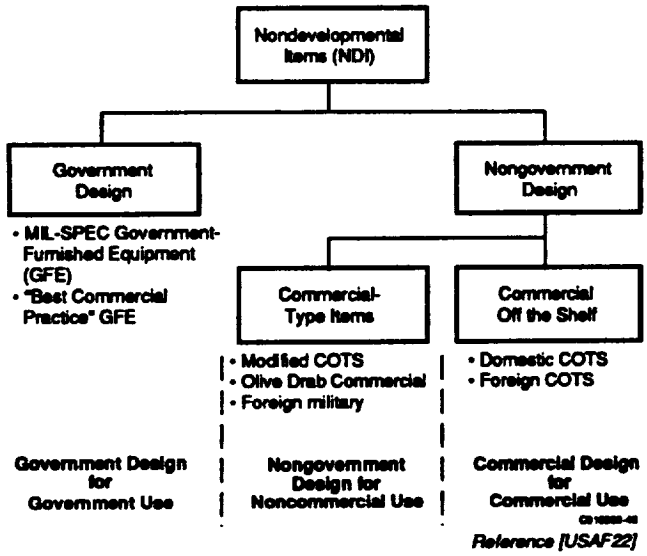


Figure 1-1. Commercial Spectrum Flow Chart

Olive Drab Commercial products come from a segment of industry oriented to selling equipment to the government and willing to undertake development of militarized, semi-militarized (and similarly, space-qualified and semi-space qualified) designs at their own expense. The government obtains qualified or semi-qualified hardware without having to sponsor the development or wait for its design. These originate as nongovernment designs for noncivilian use. Because they are used only by the government, the designs are stable over time. The government, however, does not have control over the items' documentation.

MIL-SPEC hardware included within the COTS+ definition follows the classic military approach to design and construction and is usually designed for the government. The design philosophy and the selection of MIL-SPEC parts are strictly according to standards and specifications, and typically the cost and part lead time are high. Nevertheless, procurement and use of mature, MIL-SPEC hardware may provide a cost-effective alternative to using space-qualified or commercial-grade avionics for particular missions/applications.

1.4 The COTS+ Approach

This study develops a COTS+ design philosophy using different architectures, new system concepts, promising new technologies, and innovative uses of new technology. The design philosophy establishes an open architecture, allowing different network and subsystem standards to coexist. It allows a mix of COTS+ with space-qualified equipment and a mix of modular cabinets with standard, chassis-mounted equipment. From the design philosophy baseline, a strawman, point-of-departure, future manned mission architecture is presented. This architecture, its partitioning, its components and their characteristics are used to establish requirements for using COTS+ in space.

The architecture uses a mix of commercial integrated modular avionics (IMA) components and technologies with commercial/military-qualified line replaceable unit (LRU) components. Commercial aircraft IMA principles are used within this study and ARINC IMA guidelines are incorporated throughout this report. A most recent implementation of the IMA concept, the Boeing 777's Airplane Information Management System (AIMS), is used within the architecture to assess fitting commercial off-the-shelf products in space systems.

COTS+ IMA is formed around the concept of powerful computers with an operating system that allows independent processing of application software, while maintaining robust partitioning between software modules for even the most critical functions. The computers are housed in a cabinet of hardware modules, forming a subsystem with a common cabinet design, shared fault-tolerant processing, centralized power supplies, and flexible vehicle interfaces.

Several of these cabinets interconnected by ARINC 629 and Fiber Distributed Data Interface (FDDI) global data buses connect avionics hardware outside the cabinet, forming an integrated system for performing all avionics functions on the vehicle. The hardware acts as an electrical interface, while the aircraft functions are mostly, and sometimes entirely, implemented in software modules. Software partitioning and structuring are important to this concept. A rigorous process is necessary for defining software modules and maintaining their integrity.

High-throughput microprocessors, the Ada programming language, the FDDI network, the ARINC 629 data bus and efficient power distribution are the key components and technologies necessary to design, develop and integrate this type of advanced avionics architecture.

The interface to the outside world (e.g., transducers, sensors, actuators, displays, controls and radio frequency transmitters/receivers) is handled by components external to the cabinets but is controlled by and embraced by the total COTS+ integrated modular avionics design. Cost-effective ARINC 449 data buses and serial Taxi buses are used for these interfaces.

1.5 History

Since the mid 1980s, the commercial air transport industry has been investigating ways to exploit new technologies for the purpose of developing smaller, lighter and more cost-effective avionics systems. Advancements in technology, specifically in the areas of microelectronics, fault tolerance, and software, have enabled the aircraft avionics industry to develop new design concepts that result in highly integrated digital avionics under software control. This approach, collectively referred to as integrated modular avionics, introduces methods that result in substantial cost savings compared with earlier avionics implementations.

The emerging dominance of software added yet another reason to redefine the aircraft avionics suite. Beginning in 1986, the Airlines Electronic Engineering Committee (AEEC) and the AEEC Systems Architecture and Interfaces (SAI) Subcommittee held meetings at which representatives from academia, government, avionics manufacturers, airframe manufacturers, and airlines discussed how new technologies could benefit future generations of aircraft avionics.

In 1988, representatives of the NASA Langley Research Center briefed the SAI Subcommittee concerning the application of fault-tolerant avionics to commercial aircraft. Later in 1988, AEEC adjusted the work program of the SAI Subcommittee to focus specifically on future systems. AEEC recommended the development of a top-level IMA design guide from which ARINC Report 651, "Design Guidelines for Integrated Modular Avionics," was generated.

ARINC Report 651 on Design Guidelines for Integrated Modular Avionics contains the underlying principles and concepts necessary to design and implement integrated modular avionics. A significant amount of the study document herein is derived from the draft of Report 651. The authors of this study acknowledge and appreciate the use of ARINC Report 651 information and the permission to incorporate IMA guidelines by the AEEC.

Boeing Company officially launched the 777 airplane program on 29 October 1990, and first delivery is expected in 1995. The 777 avionics were designed to incorporate IMA concepts and include several new features.

Some of the new features provided by the 777 include a fly-by-wire system, flat-panel displays, ARINC 629 network buses, SAFEbus™ backplane buses, and the AIMS. The 777 avionic architecture provides greater flexibility for future growth by taking advantage of new technology without architectural changes and accommodates system upgrades without hardware changes. Boeing 777 architecture and the above listed features are assessed in this report for their suitability for future manned mission applications.

1.6 Study Methodology

This study is initiated recognizing recently stated executive branch, legislative committee, and space community desires to explore innovative concepts, greatly improve national launch capability, reduce space operation costs, and improve space system reliability, responsiveness, and mission performance. Guided by these national space program objectives, this study seeks to apply commercial avionic products from Airbus, MD11, and Boeing 777 and military aircraft, etc., to present and future space avionics systems. The study thrust is to answer two key questions:

- Will commercial avionics do the job in space?
- What improvements are needed?

The study outline shown graphically in Figure 1-2 identifies six major tasks to be performed. These are:

- Identify COTS Avionics—Commercial off-the-shelf products (components, equipment, and technologies) applicable for space avionic applications will be identified. The product characteristics and attributes will be cataloged in a data base. Emphasis will be placed on identifying each product's environmental qualifications.
- Requirements Definition—The space mission will be defined to determine avionic performance, quality, and architectural requirements.
- Architecture Definition—A COTS+ architectural framework will be developed to illustrate the COTS+ concept and serve as a strawman architectural configuration for assessment and comparison with other configurations, including systems employing 100% space-qualified components. The strawman architecture will represent a bottom-up approach to incorporating commercial products in space applications.
- Review Lessons Learned—A review of past programs and studies will be conducted to ensure that requirements are compatible with lessons learned and current concepts.
- Identify Technology Needs—Space mission requirements and COTS+ characteristics are compared to determine modifications to space requirements, COTS+ architecture, and/or COTS+ products (see Figure 1-3).
- Development Recommendations—Development directions and recommendations are presented based on identified technology needs.

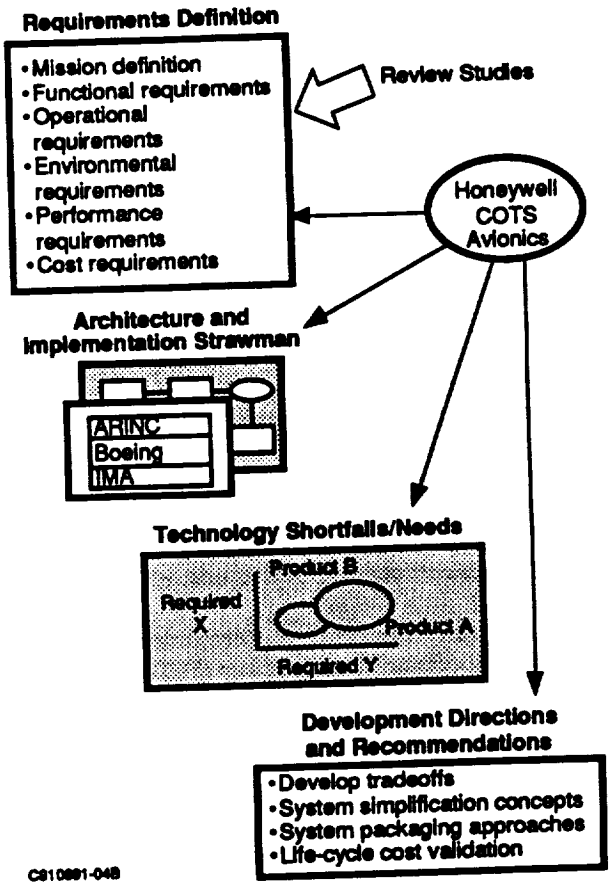


Figure 1-2. Six Major Tasks to be Performed

1.7 Report Organization

This document is organized into eight sections and two appendices, which discuss economic, technical, and administrative issues associated with the design of IMA.

- The **Executive Summary** presents a summary of conclusions and recommendations for the implementation of COTS+ in space.
- **Section 1** introduces the document and provides background information leading to its development.
- **Section 2** presents the key economic and operational objectives for COTS+.
- **Section 3** establishes the requirements applicable to future manned missions.
  - **Subsection 3.1** describes the future manned mission and vehicles.

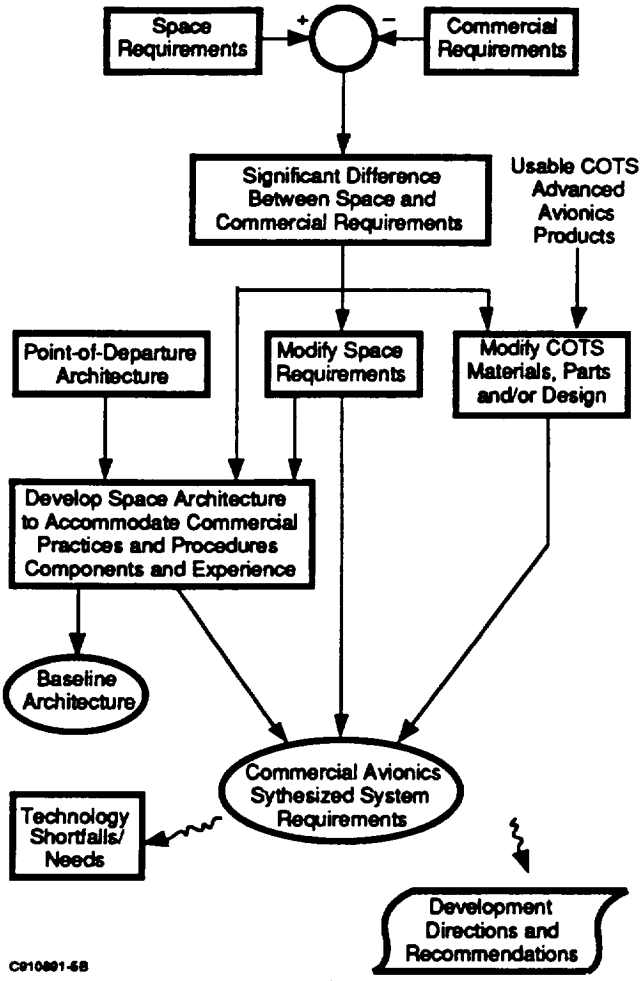


Figure 1-3. Technology Needs Comparison

- **Subsection 3.2** generates avionic requirements.
- **Subsection 3.3** addresses certification considerations and provides guidance to designers and regulatory authorities. It also reviews accepted industry philosophy and general recommendations intended to minimize the complexity of certification.
- **Subsection 3.4** recommends testability and maintainability concepts that should be applied to the design of IMA components and their implementation.

- **Section 4** describes COTS+ architecture. This subsection addresses several architectural components and issues:
  - **Subsection 4.1** defines the domain of commercial components evaluated in this study.
  - **Subsection 4.2** identifies supporting technologies and standards forming the foundation of the COTS+ concept and describes pertinent ARINC reports and specifications fundamental to the IMA concept.
  - **Subsection 4.3** addresses system architecture. This subsection describes an architecture promoting a high level of hardware integration while ensuring integrity. All space vehicle functions are included.
  - **Subsection 4.4** describes the data communications network for handling large amounts of data on the vehicles.
  - **Subsection 4.5** provides guidance for the application of fault-tolerant principles for the purpose of meeting COTS+ integrity and maintenance objectives.
  - **Subsection 4.6** describes goals for software design and programming.
  - **Subsection 4.7** provides guidance on the design of functional source and output devices such as RF equipment, air data probes, actuators, nondigital sources and data concentrators.
- **Section 5** discusses COTS+ technology shortfalls and needs.
- **Section 6** suggests development direction and recommendations.
- **Section 7** includes note, definitions, and acronyms/abbreviations.
- **Section 8** contains the references used in preparing this report.
- **Appendix A** describes COTS+ components and technology.
- **Appendix B** contains supporting viewgraphs and annotations.

1.8 Relationship to Other Documents

The material in this report is intended to complement all ARINC and AIMS characteristics and specifications referenced in Subsection 4.4. To avoid inconsistencies and discrepancies, some subjects have been omitted since ARINC documents or other specifications on those subjects are known to exist.

It is also the intent of this report to encourage the use of any standards of good practice developed by the Government, the military, and other industry groups that are applicable to COTS+ electronic equipment.

Section 2
Objectives

2.1 Introduction

This section describes the key goals and objectives for the design, implementation, and service of Space Candidate COTS+ products. These include program objectives, design objectives, cost objectives, and the desire for integration, interchangeability, reliability, and maintainability of avionics.

COTS+ objectives include new program-level ideas, methods, processes, architectures, and requirements describing how commercial products such as discrete sensors and probes, computers, displays, connections and wiring, software, support equipment, and technology can best be applied in a manageable way.

COTS+ emphasizes a program-level systems approach to engineering, recognizing that future manned missions present a new set of challenges in systems design. High levels of autonomy are required of the initiative, and systems must provide high levels of reliability and operability [JOHN90].

To achieve these goals in the face of great complexity, various organizational techniques, new technologies, creative concepts, and prudent use of cost-effective COTS+ components must be explored. It is the intent of this study to investigate and disclose measures that can be incorporated to attain these goals.

The motivations and expected goals of COTS+ in the context of total life-cycle costs, i.e., vehicle first-cost, operational costs, costs of changes and additions, maintenance and training costs are described. Attempts are made to categorize the benefits as they pertain to integration, fault tolerance, and modularity. Both direct and indirect benefits of applying COTS+ and commercial IMA standards/precepts to future aircraft systems are described.

2.2 COTS+ Benefits

The goal of using COTS+ in space is to satisfy the objectives of users and operators of the technology; the vehicle manufacturers that design, build, and support spacecraft; and equipment manufacturers that contribute to the innovative design, efficient production, and support of the components and subsystems. User benefits include reduced life-cycle cost through:

- Increased operational performance, reduced empty weight, increased payload volume;
- Increased performance by using the most recent technology;
- Reduced unscheduled maintenance and spares requirements;
- Simplified service life changes and additions to the avionics;
- Dependability from designs flown for thousands of hours in commercial aircraft;
- Increased mission opportunity and availability of avionics.

Benefits to the vehicle manufacturer include reduced first-cost and cost of service life support of the vehicle through:

- Reduced development, certification, and production costs;
- Flexibility to efficiently meet customer requirements and to implement improvements.

Benefits to equipment manufacturers include increased marketing opportunities of specialty components and subsystems through:

- Increased market volume,
- Longer production runs,
- Flexibility to efficiently meet customer requirements.

2.3 Operational Objectives

COTS+ integrated modular avionics is expected to allow the avionics equipment to take full advantage of technology changes and to expand efficiently. It is an objective to design in a capability to upgrade systems and to add new functions through on-board software loading of revised application programs or new ones.

2.4 Design Goals

Once the desired functional performance, operational objectives, and safety are achieved, then the cost of ownership over the life of space vehicles is the primary criterion against which a system is judged.

Cost of ownership should be used to trade off all other factors. The designer should provide avionics in which the sum of all contributing cost factors—development, amortization, materials, spares, weight, volume, operation, maintenance, test equipment, growth, etc.—is minimized over the life of the aircraft. It is not acceptable to reduce one cost factor and neglect others. In particular, it is not acceptable to favor first-cost effects over continued life-cycle costs. Cost of ownership models should be developed and be kept current for use in avionics upgrade programs and new development programs.

2.4.1 Goals of Integration

The system design should make maximum use of shared resources to keep resource duplication to a minimum. Such integration lowers the cost of ownership by reducing the acquisition cost, spares requirements, weight, and volume of the avionics equipment.

While hardware integration is desired, software functional independence is essential, and a certifiable method for partitioning these independent software elements from each other is necessary. Hardware integration is often limited by the desire to minimize complexity and prevent unreasonably high spare unit costs.

System-level integration of COTS+ products/technology with space-qualified products/technology is desired. COTS+ architectures should allow a mix of avionics designed for space with COTS+ products/technology. This backward integration would provide for the coexistence of COTS+ with contemporary space vehicle architectures.

2.5 Dependability Goals

2.5.1 Fault Tolerance and Redundancy

The approach to redundancy in a commercial IMA system is viewed on two levels: functional redundancy and component redundancy.

*2.5.1.1 **Functional Redundancy***—In a COTS+ system, functional availability is ensured by providing multiple paths for the data from its source to the processing required to the sink for the data, whether an indicator, actuator or other function. Although functional redundancy uses duplication of component strings, emphasis is placed on the use of fault containment techniques to allow other components in the system to continue functioning in the presence of failures.

*2.5.1.2 **Component Redundancy***—Component redundancy can play a major role in assuring mission probability of success for extended duration missions (e.g., the Mars transfer/excursion missions). In the COTS+ integrated modular avionics approach, component redundancy is implemented at the lowest line replaceable module (LRM) level. Ultra-high system reliabilities can be achieved if a pool of cold-spare LRMs is used for replacement of failed redundant components. Without this cold-spare capability, ultra-high reliability (i.e., fail-operative, 10-failure probability) would be impractical using traditional redundant-string architectures. This study presents COTS+ architecture and maintenance procedures acceptable, as a goal, to the space community.

2.5.2 Transparency

The level and the physical method of redundancy used in each of the components is to be totally transparent to the application software. Hardware shall be designed independently of the application software so that changes in either do not affect the other.

A detailed interface definition makes this approach possible. Standard interfaces are specified to allow competing or dissimilar designs to be used in different cabinets without affecting the design of the application software. This minimizes the validation effort required and allows equipment manufacturers to have flexibility in the design of their equipment. Only the integrity of the integration has to be verified each time either the hardware or software changes. Separation of the physical and application design allows the hardware and software to develop and mature at their own rates.

2.6 Maintenance Operations

The commercial IMA maintenance philosophy is built upon the desire for scheduled maintenance intervals, whereas spacecraft maintenance must be coordinated with opportunities to access the vehicle/avionics. Although maintenance operations for commercial aircraft and space vehicles seem different, IMA maintenance requirements conveniently fit within the COTS+ maintenance philosophy.

2.6.1 IMA Maintenance Philosophy

Scheduled maintenance is possible if the system maintains operational capability in the presence of faults, which implies deferred maintenance. Therefore, to achieve scheduled maintenance for commercial aircraft, it is necessary to (1) identify and contain faults, and (2) provide resource redundancy until maintenance actions are performed.

2.6.1.1 Fault Containment—To achieve scheduled maintenance for commercial aircraft, fault-containment areas must be established throughout the architecture. With this approach, it is possible to quickly detect any failure and isolate it to a given fault-containment area. A very high percentage of faults must be detected. Each of these fault-containment areas detect and annunciate the validity of its data to all users of that data. This way the system accurately reports the status of its own health and enables users to achieve the maintenance goals that were previously unattainable. It is a goal to make all commercial first failures transparent to the flight crew, annunciate first failures to the maintenance crew, and allow maintenance to be scheduled at a convenient time.

2.6.1.2 Resource Redundancy—Some level of resource redundancy must be provided to extend the mean time between maintenance alert/action (MTBMA). The resource redundancy required to extend the MTBMA is dependent upon the length of the extended maintenance interval and the statistical probability of successfully completing that interval before total equipment failure. Resource redundancy may be made available through secondary redundancy at the component level, or it may be made available at a system level, as part of the aircraft architecture, by automatic reconfiguration.

As guidance, IMA has established that, for a fully fault-tolerant avionics suite, the mean-time-to-maintenance-alert goal for an individual avionic function is at least 15,000 hours. Furthermore, it is desired that the full avionic function continue to be available for 200 hours after the first fault with a 99% probability of success. The overall system architecture design will contribute to the reliability goals for each avionics function. It is a design objective of IMA to apply this maintenance philosophy to all aircraft systems, including sensors and aircraft wiring.

2.6.2 COTS+ Maintenance Philosophy

It is a COTS+ objective to use commercial IMA scheduled maintenance concepts and requirements to incorporate deferred maintenance (i.e., fly without repair) concepts during extended flight. Furthermore, COTS+ attempts to incorporate deferred maintenance for expendable launch vehicles using COTS+ technology (this is recommended for future study). Although no deferred maintenance requirement specified by Multi-path Redundant Avionic Suite (MPRAS) or by the commercial ARINC 651 IMA guidelines, deferred maintenance philosophy will be presented within this COTS+ study.

MPRAS Technical Memo TM-1 did not recommend deferred maintenance for launch vehicles since projected savings did not justify the cost of implementing an added level of high-confidence avionics redundancy for deferred maintenance. However, TM-1 did not consider the cost savings of implementing vehicle avionics with COTS+ technology. Further studies are recommended to assess deferred maintenance using COTS+ technology in expendable launch vehicles.

The ability to employ fault tolerance to defer maintenance actions is not required, detailed, or stipulated within the IMA guidelines. It is mentioned only as an attraction concept. IMA ojectives, however, imply the use of deferrred maintenance.

Deferred maintenance using component redundancy will be required to support extended-duration and/or deep-space manned missions. During these extended missions, replacement of failed components is expected within the COTS+ philosophy. Crew workloads will not always allow immediate repair or replacement of equipment after failures. It is a goal to make all COTS+ first failures transparent to the flight crew, annunciate first failures to the maintenance personnel, and allow maintenance to be scheduled at a convenient time within approximately four days.

Essential deferred maintenance building blocks will be established within this study.

2.6.3 Goals of Modularity

The primary goal of using commercial modular avionics is to reduce the cost of ownership through lower acquisition cost and to increase flexibility to accommodate variations. Modular avionics are designed to reduce the total cost of spares inventory by making the replacement elements as small a part of the system as practical. Acquisition costs are reduced by allowing high-volume elements to be separately produced, thus achieving economies of scale. Avionics development costs will also be reduced since standard interchangeable modules can be used in a variety of commercial aircraft and space vehicle types without modification.

2.7 Equipment Packaging and Location

2.7.1 Weight and Volume Considerations

Generally, users agree that equipment should be as lightweight and compact as possible, and integration techniques should be used to minimize equipment size and weight. However, the desire for compact lightweight equipment should not result in packaging designs that result in high-cost spares (e.g., custom I/O modules) and compromise overall system integrity or life-cycle costs. It is within this objective that COTS+ avionics is superior to equipment designed specifically for space.

The desire for compactness should not cause thermal rise problems that can be solved only by exotic cooling methods or require otherwise unnecessary radiation shielding within avionic chassis or compartments. The packaging designer should work closely with the system designers to evaluate the tradeoffs of small, lightweight designs.

2.7.2 Location and Accessibility of Components

The trends toward small, lightweight equipment with high mean time between failures (MTBFs) and toward the use of the ARINC 629 data bus provide the freedom to distribute equipment on space vehicles in a variety of locations. Equipment location should be determined based on a number of factors listed below. It is the system integrator's responsibility to analyze these factors before distributing equipment on the aircraft.

- Function and operational performance;
- Environment concerns;
- Access for maintenance;
- Maintenance philosophy;
- Integration with other systems;
- Growth potential and access for modifications;
- Lengths, number of wire runs, and number of interconnects with source systems.

Equipment with expected low MTBF with respect to other equipment should be mounted in a location that affords easy access. For manned vehicles, the designer should consider locating major COTS+ equipment in the cockpit, cabin wall, cabin overhead, or other areas that are easily accessible.

In all cases, a time-to-replace analysis should be completed for each LRU or LRM in its respective location. Equipment with expected high MTBF can be located in areas where the access is limited as long as an analysis of failure rate in relation to time-to-replace is within acceptable limits. High-MTBF equipment can be mounted in a manner that involves an acceptable level of difficulty to remove the equipment.

Special tooling to remove equipment or locking mechanisms should be used for equipment with a moderate to high level-of-removal/replacement difficulty. Consideration should be also be given to automated mechanisms designed to remove both low- and high-MTBF equipment with controlled sequences, forces, and handling.

2.8 Interchangeability

One of the continuing goals of both airline users and aircraft manufacturers is interchangeability of avionics equipment manifested with interoperability and open architecture specifications. Interchangeability is necessary to achieve economies of scale, to distribute design and development costs and to reduce the spares inventory. Ideally, interchangeability can be applied to any manufacturers' components and between any two aircraft types and models. This has been achieved often enough in the past to prove that interchangeability is a feasible goal.

A COTS+ goal is to provide interchangeability of COTS+ equipment with equipment similar to COTS+ equipment or space-qualified equipment with the same function.

2.9 Spares Provisioning

Spares provisioning is based on maintenance plans developed for a particular vehicle and the extent that it is adapted to meet the needs of a particular mission. The COTS+ objective is to require the fewest number of spares without jeopardizing flight safety.

2.10 COTS+ in Flight Simulators

Flight simulators and maintenance trainers are now recognized as an essential part of the aerospace industry. We have become increasingly dependent on such simulators for flight crew and maintenance crew training. Users typically require these simulators to be available as early as possible to allow for crew training before equipment introduction into service.

As part of the design and construction of these devices, simulator manufacturers simulate many avionics LRU/LRMs. However, such equipment simulation is not practical nor desirable in many cases; therefore, the use of an actual avionics unit within the flight simulator is required. The flight and operational environment for stimu-

lating the avionics equipment is programmed in the simulator host computer. The currency of spacecraft avionics software is maintained through updates and procedures similar to those adopted for the aircraft.

The need for ever-increasing levels of fidelity and credibility has forced the use of unmodified avionics in flight simulators. These avionics, when subjected to the environment of flight simulators, have exhibited a tendency to behave abnormally as a result of the execution of simulator functions such as freezes, repositions, resets, and slews.

The disruptions caused by the unwanted side effects of the simulator functions on the avionics slow down the training process. Special work-around procedures must be established to bypass the problems; alternatively, additional explanations have to be provided to describe the differences between the simulator behavior and the spacecraft behavior, which greatly increases training costs to the airlines. As a general rule, within reason, designers should avoid defining hardware and/or software architectures or algorithms that are incompatible with the simulator functions.

Section 3
Requirements

To integrate COTS+ within space, it is necessary to know COTS+ avionic environments, functional needs, and performance requirements. Of the three, COTS+ avionic environments plays the most significant role in the assessment of COTS+ in space. To succeed in the space integration of COTS+, it is critical that there be a match of COTS+ environmental capabilities and space avionic environments. This section emphasizes the generation and definition of the COTS+ environmental requirements.

Subsection 3.1 defines the COTS+ missions and vehicles. This definition is essential to the determination of the avionic environmental requirements. Environmental and performance requirements are subsequently generated and provided in Subsection 3.2, Avionic Requirements. Subsection 3.2 also summarizes program-level and mission-related requirements and presents a matrix chart that compares program-level, mission-related, and environmental requirements to future manned missions and their vehicles.

COTS+ functional and performance requirements are provided in the remainder of this document. These requirements, which relate to verification and validation, maintenance and test, standard modules, architecture, data networking, data sources, fault tolerance, and software, are derived from bottom-up COTS+ requirements. They define functions, performances, interfaces, and configurations representative of COTS+ technology. They are derived from ARINC Report 651 on Design Guidelines for Integrated Modular Avionics and the characteristics and capabilities of the Space Candidate COTS+ products and technology identified within this study. These requirements are referred to as bottom-up derived requirements because they are initially implemented without regard to top-down program/mission-level derived requirements. Eventual blending of top-down and bottom-up requirements is achieved by this study.

Credit and appreciation is given to the University of Minnesota Aerospace and Mechanics class for information on the Mars Integrated Transportation System (MITS) derived from two final reports for USRA/NASA at Marshall Space Flight Center. The class developed two different mission profiles to Mars, each with a different vehicle. This study greatly benefitted from the comprehensive presentations within their final reports [UM-A91 & UM-B91].

3.1 Missions and Vehicles

3.1.1 Introduction

To establish the requirements, it is necessary to know avionic requirements for COTS+ reference vehicles; the fact that COTS+ is applicable to many space missions and a multitude of vehicles complicates the task. Because of the many COTS+ benefits, it is a goal to apply COTS+ in as many space architectures as possible. Consideration is therefore given to integrating COTS+ within all future manned mission avionic architectures, including launch boosters, transfer and excursion vehicles, modules, and stations/platforms. COTS+ reference vehicle definitions are required for each mission. Point design reference vehicles, representative of what typical COTS+ application vehicles may be or look like, will be used as platforms to integrate COTS+ technology. They are defined for various future manned missions herein. The reference vehicles, their missions, and some of their operations are described within this section.

3.1.2 COTS+ Missions

3.1.2.1 Earth to Orbit (ETO)—The Space Transportation Architecture Study (STAS) defines a complete launch system architecture. The COTS+ Earth to Low-Earth Orbit (LEO) baseline mission includes the STAS model goals:

- A highly autonomous vehicle,
- Automated checkout,
- A high level of health monitoring integration,
- Near 100% availability,
- Increased system reliability,
- Reduction of life-cycle cost by an order of magnitude,
- Provision of 100% assured access to space,
- Significantly reduced turnaround time,
- Maintenance of world leadership in space,
- Fault tolerance,
- Standardized interfaces,
- Minimal environmental constraints.

Although there is reason to change STAS mission models, the total delivered payload mass for the option we considered was approximately 9.85 million pounds, the total returned payload mass was approximately 6.76 million pounds, and the payload value was approximately 197 billion 1986 dollars.

Launch Vehicles—The COTS+ launch booster reference vehicles shall represent vehicles of various configuration and different payload capabilities. The COTS+ booster reference vehicles represent expendable launch vehicles (ELV/ALS-E), reusable core with expendable booster(s) (ALS-FBB), flyback boosters, and Space Transportation System (Shuttle) configurations. The reference vehicles also provide variable payload lift capabilities required of STAS, lunar, and/or Mars missions.

The STAS vehicles included Titan IV and several new vehicle classes from 25,000- through 300,000-lb payload lift capabilities. The Mars excursion may require heavy lift launch vehicles (HLLVs) or two additional launch vehicle classes to place mission components in LEO [UM-A91 & UM-B91]:

- 150,000–200,000-lb Class—External tank (ET) derived in-line launch vehicle family. It will be used to place smaller components in orbit in University of Minnesota Study A.
- 200,000–300,000-lb Class—Equivalent to the the HLLV. This will be used to place most other lunar and Mars components (e.g., propulsion system, and fuel tanks) in LEO in U of M Study A. The HLLV is used to place all Mars transfer vehicle and excursion vehicle components and fuel in LEO in University of Minnesota Study B
- 300,000–400,000-lb Class—Defined by the University of Minnesota, Aerospace and Mechanics, Mars Integrated Transportation System Operations group to place the Mars transfer vehicle aeroshell in orbit in University of Minnesota Study A.

Several reference launch vehicles are illustrated in Figures 3-1 through 3-4. They represent new and old designs, are used for different missions, provide various payload capabilities, and exhibit a mix of expendable, reusable, and flyback booster configurations.

3.1.2.2 Orbit Parking—Stations and platforms such as Space Station Freedom (SSF) parked in low earth orbit shall be COTS+ integratable. SSF's mission, operations, and structure can be found in a number of references (e.g, [SPAC84]).

3.1.2.3 Orbit Transfer, Transit, and Excursion—COTS+ architecture shall be used for the following future manned navigational missions:

- Orbit transfer missions—LEO to high earth orbits (geosynchronous, geostationary, Molnia, etc.);
- Lunar and Mars transfer vehicle missions (solar navigation);
- Lunar/Mars excursion missions.

These vehicles will be for crew and cargo transfer.

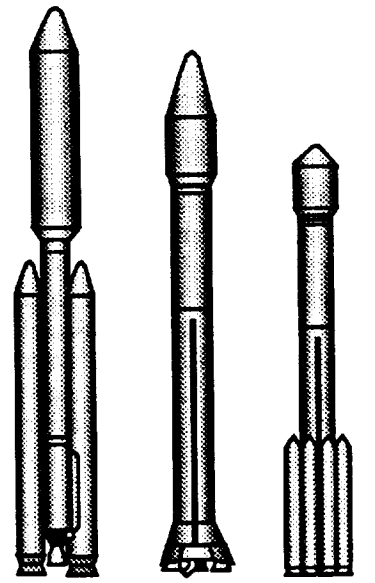


Figure 3-1. Expendable Launch Vehicles (ELVs)

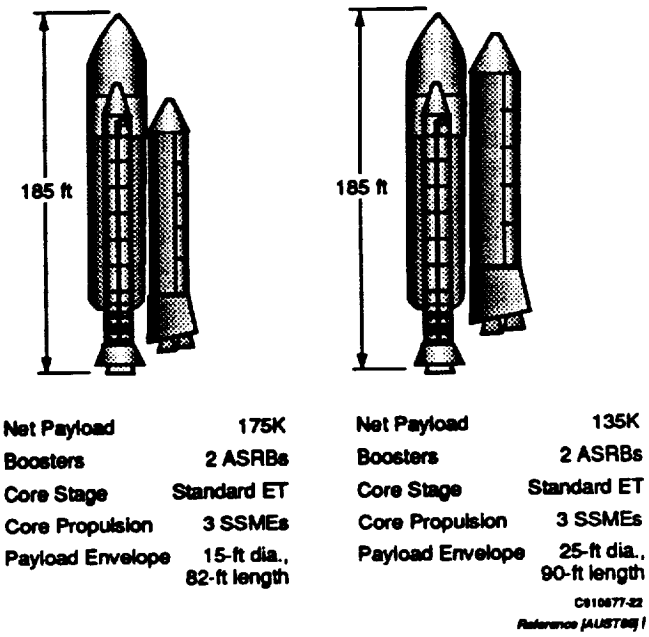
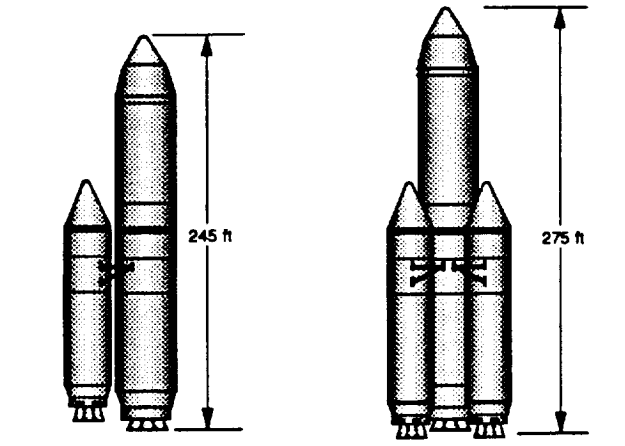


Figure 3-2. Shuttle-Derived Vehicles for LEO and Lunar Missions

OTVs, LTVs, MTVs, and Excursion Vehicles—Orbital transfer vehicles (OTVs), lunar transfer vehicles (LTVs), and Mars transfer vehicles (MTVs) are illustrated in Figures 3-5 through 3-9. They represent the COTS+ reference vehicles of this study.



Net Payload	115K	Net Payload	215K
Boosters	3 LOX/LH_2 with 6 STMEs ea.	Boosters	2 LOX/LH_2 with 6 STMEs ea.
Core Stage	LOX/LH_2	Core Stage	LOX/LH_2
Core Propulsion	3 STMEs	Core Propulsion	3 STMEs
Payload Envelope	25-ft dia., 100-ft length	Payload Envelope	40-ft dia., 100-ft length

C910877-03
Reference [AUST89]

Figure 3-3. Advanced Launch System (ALS) for Lunar and LEO Missions

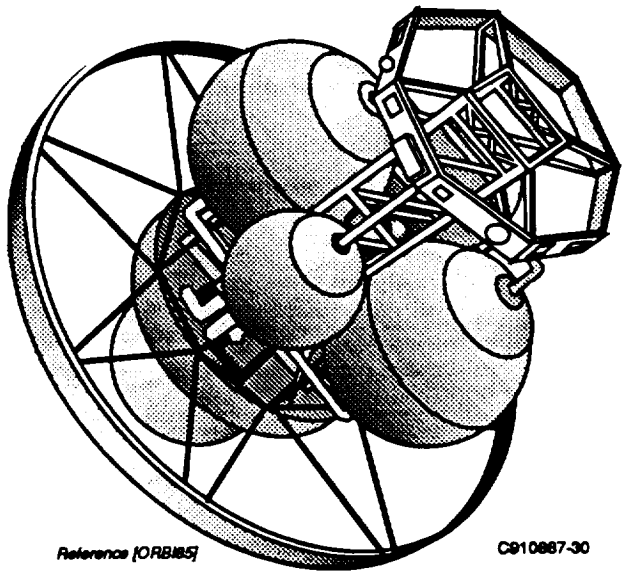
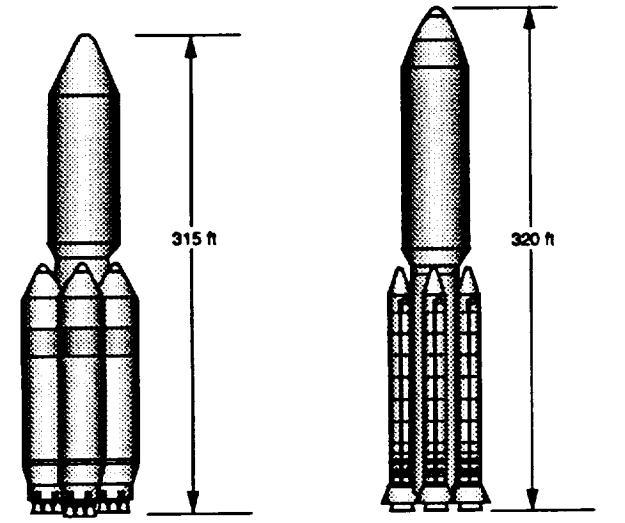


Figure 3-5. Orbital Transfer Vehicle



Net Payload	300K	Net Payload	300K
Boosters	3 LOX/LH_2 with 6 STMEs ea.	Boosters	4 ASRBs
Core Stage	LOX/LH_2	Core Stage	New 30-ft dia.
Core Propulsion	3 STMEs	Core Propulsion	Recoverable P/A with 5 SSMEs
Payload Envelope	40-ft dia., 100-ft length	Payload Envelope	40-ft dia., 100-ft length

C910877-01
Reference [AUST89]

Figure 3-4. HLLV for LEO, Lunar, and Mars Missions

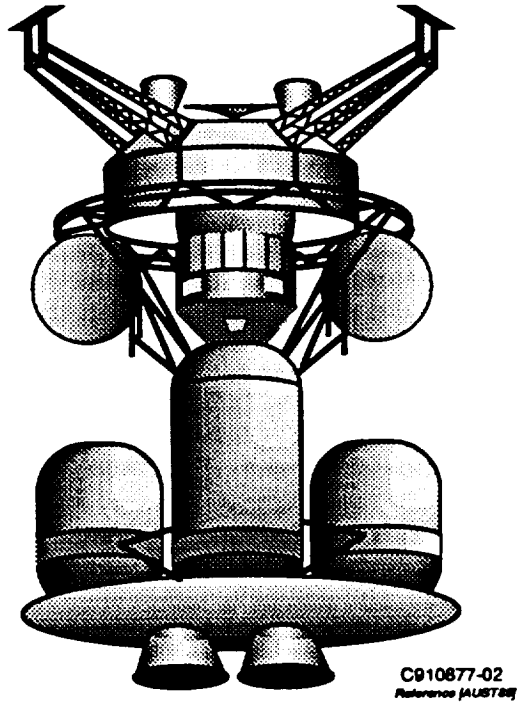


Figure 3-6. Lunar Transfer and Excursion Vehicle

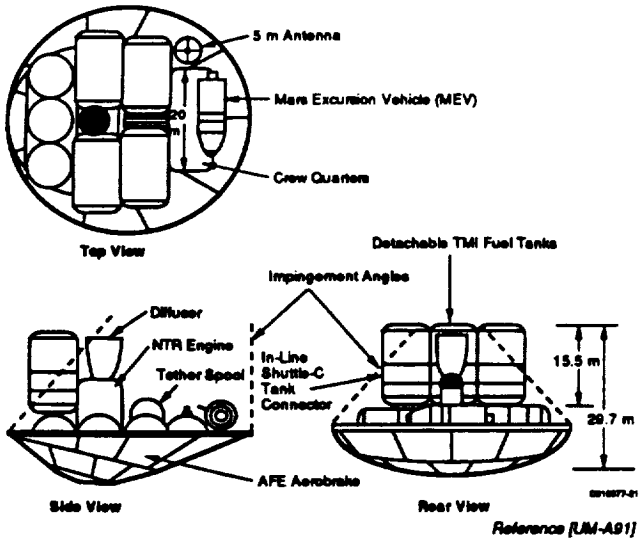


Figure 3-7. Mars Transfer Vehicle

3.1.2.4 Habitation Environment—The COTS+ concept shall be integratable within lunar and/or Mars surface missions. The avionics for the modules shall provide power generation and control, communications, environmental control, etc., typical of avionic requirements for orbiting platforms. A diagram of a typical Mars habitation module is shown in Figure 3-10.

3.2 Avionic Requirements

3.2.1 Introduction

COTS+ avionic requirements based on top-down program-level, mission-level, and vehicle-level requirements are presented herein. Avionic requirements for COTS+ reference vehicles are first determined using published characteristics of past, present, and envisioned space vehicles to establish upper and lower requirement limits. Requirement restrictions imposed by COTS+ products and integration are then used to modify the avionic architecture and requirement specifications of this section.

3.2.1.1 Background—The space program continues to use old and modified/upgraded vehicles and plans to build families of new vehicles for various missions. To be cost-effective, COTS+ must be valid for vehicle upgrades (backward integration) as well as for new applications.

A literature search was therefore performed to obtain data on past, present, and envisioned space vehicles. From the descriptions of these vehicles, their anticipated missions, and their specified environmental requirements, a database of avionic requirements was generated.

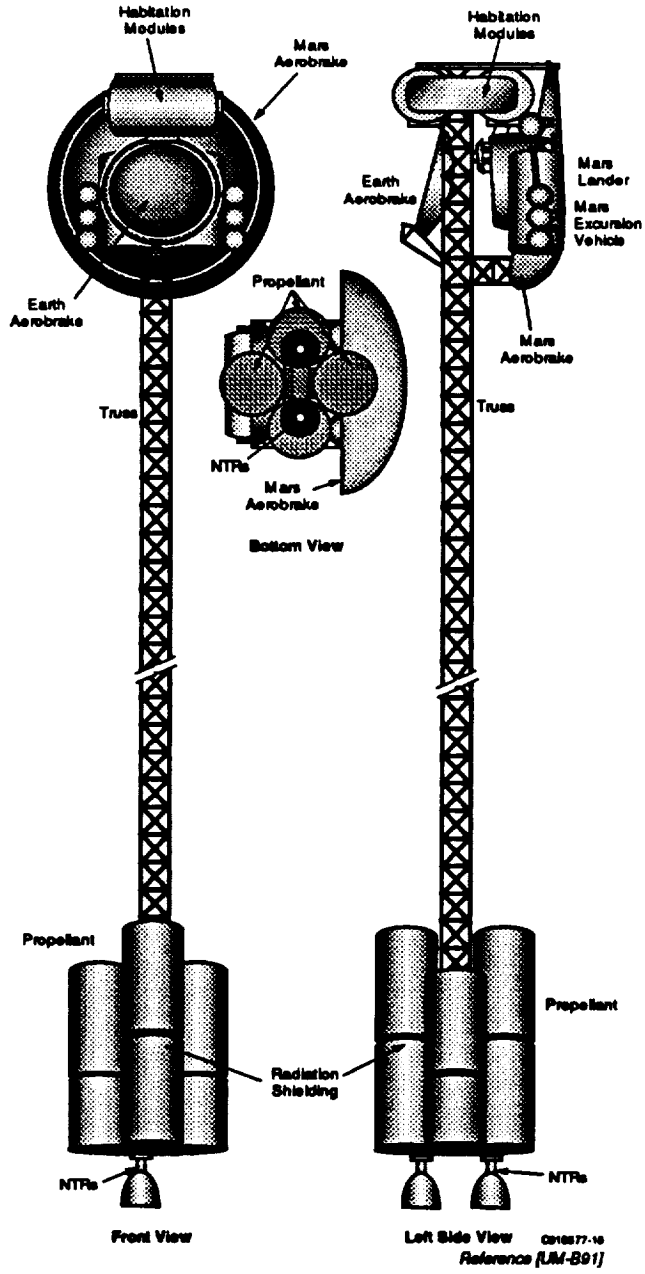


Figure 3-8. Mars Transfer Vehicle

These requirements can be compiled to establish a set of worst-case composite requirements, or can be left as is and used as a requirements database for each vehicle. An advantage to compiling data into a single composite requirement set is the simplicity of integrating COTS+ products in space. On the other hand, opportunities to incorporate COTS+ in space may be overlooked because of the more stringent requirements imposed by the composite. This study presents the requirements for several vehicles within COTS+ missions. A set of worst-case composite requirements for each of the four COTS+ missions can be derived from the data.

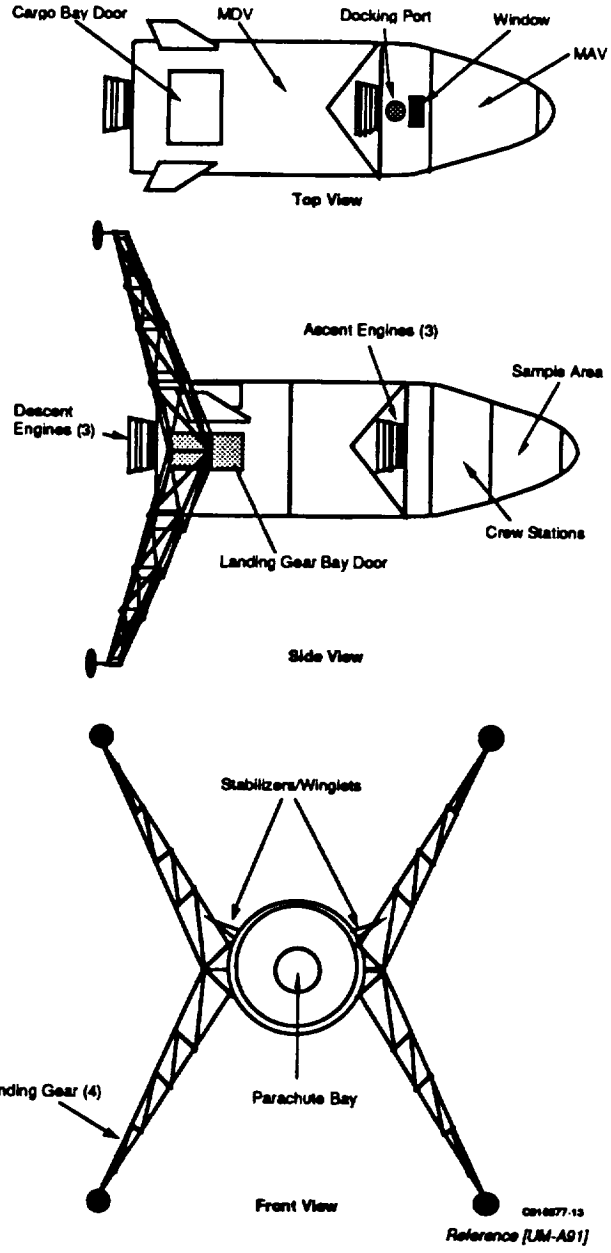


Figure 3-9. Mars Excursion Vehicle

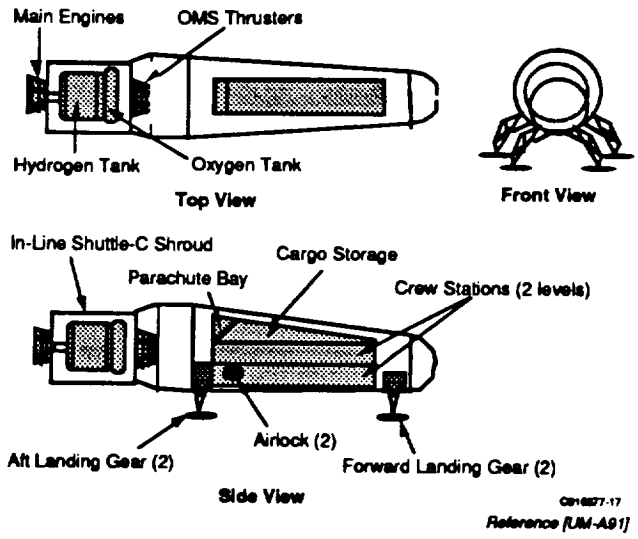


Figure 3-10. Mars Habitation Module

This subsection presents a COTS+ requirements summary table and supporting information. Discussion is limited to requirements pertinent to particular missions, vehicles, and COTS+ applications.

3.2.1.2 Requirements Summary—Table 3-1 summarizes the COTS+ mission, vehicle, and avionic requirements. Requirements are presented for each of the four primary missions: earth-to-orbit, transfer, excursion, and orbital/surface systems. The requirements for representative vehicles are presented in the table. The missions and their vehicles are as follows:

- Earth-to-orbit missions:
  - Space Transportation System (STS) Shuttle,
  - Space Transportation System - Cargo (STS-C),
  - Heavy Lift Launch Vehicle (HLLV);
- Orbital and/or surface missions:
  - Space Station Freedom (SSF),
  - Man Tended Transportation Node (MTTN),
  - Personal Maneuvering Unit (PMU);
- Transfer missions:
  - Orbital Transfer Vehicle (OTV),
  - Mars Transfer Vehicle (MTV);
- Excursion missions:
  - Lunar Excursion Vehicle (LEV),
  - Mars Excursion Vehicle (MEV).

3.2.2 Earth-to-Orbit Mission

The earth-to-orbit mission shall primarily be to deliver payloads to low-altitude parking orbits. The low-earth orbits will be used for staging to higher orbits, transitions to inter-solar-system travel, and construction of interplanetary vehicles.

3.2.2.1 ETO Durations—The mission duration for expendable components, ASRBs, liquid boosters, and liquid engine core stage is 0.5 hr. Although the boost phase is less than 20 min, 0.5 hr is selected to include prelaunch pad operations after final avionics checkout.

STS-C missions are two days on orbit, and the orbiters are to be reused over a 20-year period.

3.2.2.2 ETO Environments—Launch vehicle user handbooks specify pertinent parameters such as acoustic, vibration, and shock levels. Transporting the spacecraft from

point to point on the earth may subject it to more damaging vibration and shock than the launch [GRIF91].

ETO Vibration Environment—

Space Shuttle—Space Shuttle vibration environments are illustrated in Figures 3-11 through 3-13. The first two figures are predicted environments for (1) an unloaded main longeron trunion fitting and (2) an unloaded keel fitting, and the third presents flight data for longeron vibration based on shuttle flights STS 1–4. Flight data yielded higher frequency contents and higher Y-axis levels than predicted. The Z-axis spectral density was 0.60 g^2/Hz and extrapolates to 0.001 g^2/Hz at 10,000 Hz.

The shuttle avionics aft bay overall acceleration is 4.88 g rms from 20 to 2000 Hz.

SSMEC—The Space Shuttle Main Engine environment [CONT73] is as follows:

- Decaying sinusoidal vibration: 5–44 Hz at 0.12 in. double amplitude displacement, 44–1140 Hz at 12 g peak, 1140–1620 Hz at 0.00018 in. double amplitude displacement, 1620–2000 Hz at 24 g peak.

- Random vibration: 20–1300 Hz at 0.15 g^2/Hz, 1300–1650 Hz +18 dB/octave, 1650–2000 Hz at 0.6 g^2/Hz.

Other Vehicles—Ariane, Atlas-Centar, Delta, and Titan vehicle vibration environments are shown in Figures 3-14 through 3-20. These profiles give an indication of general launch vehicle vibration environments.

Composite—The ETO vibration environment is considered "High." From the above, rough order of magnitude (ROM), worst-case composite avionics vibration requirements (excluding engine environments) would be:

- Sinusoidal longitudinal (thrust axis) vibration: +6 dB/octave to 2 Hz, 1.5 g peak to 15 Hz, 3.8 g peak 15 Hz to 25 Hz, 1.5 g peak to 200 Hz, assume –6 dB/octave beyond 200 Hz.

- Sinusoidal lateral vibration: First stage or near engines, +6 dB/octave to 2 Hz, 1.5 g peak to 18 Hz, assume 1.0 g peak to 100 Hz, –6 dB/octave beyond 100 Hz. Second-stage flight 1.0 g peak from 4 Hz to 18 Hz and 0.6 g peak from 18 Hz to 200 Hz.

- Random vibration: +12 dB/octave to 30 Hz, 0.20 g^2/Hz to 1000 Hz, –6 dB/octave beyond 1000 Hz. The effective acceleration for the composite is rather high (24 g rms).

COTS+ Capability—From samples of commercial aircraft vibration test envelopes, the following specifications represent Civil Market COTS avionic vibration requirements for equipment mounted rigidly on airplane structures in forward fuselage, electronic bays:

- Sinusoidal vibration: 0.9 g peak to 15 Hz, –6 dB/octave beyond 15 Hz.

- Random vibration: 0.02 g^2/Hz to 20 Hz, –6 dB/octave to 45 Hz, 0.004 g^2/Hz to 1000 Hz, –6 dB/octave beyond 1000 Hz. The overall acceleration is 2.5 g rms.

It is obvious that Civil Market COTS products (commercial products purchased exactly as found) will not meet space vibration requirements unless the products are ruggedized or are mounted on secondary electronic racks. Tertiary structures may be necessary to provide the vibration attenuation factor necessary to match Civil Market COTS or COTS+ product capabilities to launch vehicle vibration environments. Distributed aircraft architectures are used to considerably reduce acceleration spectral density and overall acceleration requirements. Typical modern aircraft acceleration spectral density at 130 Hz varies from 0.002 to 1.2 g^2/Hz, and overall acceleration varies from 2.0 to 13.5 g rms for different locations on the airplane.

However, some militarized Olive Drab Commercial and MIL-SPEC products are able to meet the composite launch vehicle vibration requirements.

COTS+ Vibration Requirement—It will be a COTS+ baseline requirement to provide vibration attenuation using physical structures, physical partitioning, and the distribution of Civil Market COTS products to locations where vibration environments are within their operating envelopes.

ETO Acceleration Environment—HLLV accelerations levels are considered "High." Linear acceleration requirements are ±20 g, and the maximum angular acceleration requirement is ±100 deg/s. Shuttle vehicle applied acceleration loads, however, are considered "Low," with 2.0 g steady and ±2.0 g dynamic in landing, and 1.7 g steady and ±4.0 g dynamic at launch release (within 2 sec of release).

COTS+ Capability—Civil Market COTS product requirements derived from aircraft avionic requirements are as follows:

- Angular rates of ±100 deg/s,
- Angular accelerations of ±10,000 deg/s^2,
- Linear accelerations of ±6 g.

The disparity in linear acceleration is to be accommodated by requiring COTS+ products to meet additional testing requirements.

FOLDOUT FRAME

Table 3-1. COTS+ Mission,

◆ Mission • Vehicle - Avionics	Operations	Duration	Acceleration	Acoustics	Vibration	Shock	Pressure	Temperature	Radiation	
◆ Earth to Orbi										
• STS - Avionics	Integration, pre-launch, launch, payload delivery, docking, refurbishment	0.5-hr boost Reuse over a 20-year period On orbit: several days on orbit	± 4 g dynamic at launch release, 2 g steady at landing	174 dB for SSME near field	0.9 g peak to 15 Hz 0.60 g^2/Hz 4.88 g rms from 20 to 2000 Hz	20 g in aft avionics bay	10^{-3} Torr for SSMEC	-62° to 65°C in avionics bay	10 protons/cm^2 / day with 150 MeV energy	SSM witho usefu years
• STS-C - Avionics	Integration, pre-launch, launch, payload delivery, docking, refurbishment	0.5-hr boost On orbit: 2-day mission			High	High			Medium	Systen Avionic (10% c
• HLLV - Avionics	Integration, prelaunch, launch, payload support, payload delivery, refurbishment	0.5-hr boost 20 missions Some reusable components On orbit: 2 days for each flight (5 days on pad)	Linear: ±20 g max.; angular: ±100°/s^2	139 dB (NASA acceptance for inertial upper stage components) 155 dB (MPRAS requirement)	11 g rms	1000 g at separation	10^{-10} Torr to 18 psia	Operational: -65°F to 150°F	4 rads (Si)	0.999 launch 0.98 or (launch probab Avionic is 10%
◆ Transfer • LTV - Avionics	Prelaunch; launch; deployment; SSF docking; lunar transfer, orbit, landing, prelaunch and launch; earth transfer	1–2 missions per year, 5 missions lifetime On orbit: 11 days per mission	69 m/s^2	136 dB (at launch)	Same as launch vehicle	Same as launch vehicle	0.2 lb/in^2	150°F	150-krad (Si) minimum parts capability, 75-krad (Si) ionization dose design point	Systen Avionic (20% c
• MTV - Avionics	Transport personnel, cargo and MEV from SSF to Mars orbit, transport personnel and cargo from Mars orbit to earth or SSF	10-year life 12–16 months round trip 424 days transit On orbit: 30 to 600 days (Mars)	Medium		Medium	Medium		±150°C	High Nuclear reactor possible	Systen Avionic (20% contrib

2.

FOLDOUT FRAME

Vehicle, and Avionic Requirements

Reliability	Modularity	Maintainability	Safety	Autonomy	Cost	Testability	Security	Electromagnetic Interference	Growth and Flexibility	Particle Contamination
C: 8 hours t overhaul, life of 10	Not required	Ease of service	SSMEC fault tolerance = FO-FS Design conditions shall be precluded to ensure safety	Conduct mission operations without dependence on ground support systems dedicated only to the STS	Maintenance overhaul shall not exceed 25% of original equipment cost	Reasonable access to interface Ease of servicing and maintenance	Secure communications and data transmission and reception over various RF links are encrypted Prevent compromise of classified information during processing, storing, and general handling of classified, unencrypted data Denial of unfriendly access or control while conducting classified mission operations	Meet normal manned space flight standards	20% physical space, panel and interfaces	Protect against bridging of electrical circuits
: 0.999 s: 0.9969 ontribution)				High Functions: AGN&C, system monitoring, reconfiguration						
support eliability of higher on schedule ity: 0.95) contribution (0.9999)	Standardization of hardware, software, interfaces and data buses MIL-HDBK-246A, Program Managers Guide for the Standard Electric Modules Program	Provide facilities and equipment for prelaunch, in-flight, or refurbishment monitoring and checkout Design for easy removal, repair and replacement to the lowest level practical	Range safety Man-rated safety design requirements	High Functions: AGN&C, system monitoring, reconfiguration, minimize operations costs Require far less launch support than current systems	ALS program goal: Tenfold cost reduction (current costs range from $5000 to $10,000 per kilogram)	Parts and components qualification testing: SMILSO STD 73-2C, MIL-STD-1540A	Secure communications and data transmission and reception over various RF links are encrypted	MIL-STD-1541 Meet normal manned space flight standards	High degree of flexibility to meet operational needs Accommodate changes in mission parameters late in the prelaunch sequence	Hermetic seal
: 0.99999 s: TBD ontribution)	Commonality and modularity to reduce costs and spares provisioning, optimize functional interfaces and software module allocation	BIT/IHM, on-line (in-flight) and off-line (ground) spares MTTR: 30 min internal, 6 hr external Provide facilities and equipment for monitoring and checkout Design for easy removal, repair and replacement to the lowest level practical	Manned vehicle safety design requirements	High Functions: GN&C, sequencing, systems monitoring, ECLSS, rendezvous and dock (with manual override) Minimize routine crew workload and ground support	Minimize operations-driven costs	Provide access to test points Support ground and Lunar test and checkout	Payloads responsible for their own command and data encryption	MIL-STD-1541 Meet normal manned space flight standards	Flexibility to meet the needs of various payloads	Hermetic seal Lunar soil accumulates and acts as a thermal insulator
: 0.99999 s: TBC ution)		BIT/IHM, on-line (in-flight) and off-line (ground, SSF) spares Power down one string or one cluster for remove and replace MMTR: 30 min internal, 6 hr external		High Functions: GN&C, sequencing, systems monitoring, ECLSS, rendezvous and dock (with manual override), thermal control, data management						

C910976 11x17 A

FOLDOUT FRAME 1

Table 3-1. COTS+ Mission, Vehicle,

◆ Mission · Vehicle · Avionics	Operations	Duration	Acceleration	Acoustics	Vibration	Shock	Pressure	Temperature	Radiation	Re
◆ Orbital										
· SSF · Avionics	Prelaunch, launch deployment, construction, servicing experiments and satellites, test and upper stages, national security operations, large-scale construction of space structures	30-year mission subsystems: 10-year minimum using maintenance as necessary On orbit: 30 years	Low	Low	Low	Low (docking impact)	Shirtsleeve Pressure selected to facilitate productive EVA with no pre-breathing or other operational constraints	200 K during darkness to 350 K in direct sunlight	10^7 protons/cm^2/day with 150 MeV energy A permanent platform may encounter doses up to 3000 Mrad NASA has set a 50-rad SSF environmental requirement	Syste Avio (10 con
· OTV · Avionics	Manned uprating	Reusable Space storable for extended duration Unmanned: 42 hr operational, 24 hr standby On orbit			145-dB acoustic noise for 1 min	Tolerate accumulated shock	Meet outgassing limits of NASA SP-R-0022A		SEU: no set standard; CPU goal 10^{-7} bit/day, memory goal 10^{-9} bit/day, immunity via hardware/software Radiation hardness: no set standard; module total dose goal 10^{-6} to 10^{-5} rad.	Syste Avion
· MTTN · Avionics	Service transfer vehicles in earth orbit	On orbit: 20 years	Low		Low	Low		±150°C	Medium	Syste Avion contr
· PMU · Avionics	Transport individual personnel during EVA	5-year life On orbit: 12-hr mission	Low		Low	Low		±150°C	Medium	Syste Avion contrib
◆ Excursion										
· LEV · Avionics	Transport personnel and cargo between lunar orbit and lunar surface	1–2 mission per year, 5 missions per lifetime On orbit: 4 days per mission (lunar)	Medium		Medium	Medium	0.13 nanobars	40 K–384 K	150–krad (Si) minimum parts capability, 75–krad (Si) ionization dose design point	Syste 0.999 Avion (20% con trib
· MEV · Avionics	Transport personnel and cargo between Mars orbit and Mars surface	6 days for nominal mission, 30 days for contingency planning 600 days possible lifetime (200 days, transit, 600 days on surface and return to Mars orbit)	High		High	High		–125°C to 25°C Mars surface	High High-energy cosmic radiation	Syste 0.999 Avion (20% contrib

FOLDOUT FRAME 2

:bility	Modularity	Maintainability	Safety	Autonomy	Cost	Testability	Security	Electromagnetic Interference	Growth and Flexibility	Particle Contamination
: 9999 .s: TBD ibution)	Common hardware, software and technology to enhance standardization for direct interchangability, ensure compatability, and minimize program development costs	BIT/IHM, on-line spares, partial power-down for repair (power down one string or one cluster) MTTR: 30 min internal, 8 hr external Permit repair or replacement at the ORU level Provide facilities and equipment for on-orbit monitoring, checkout, storage, replacement, repair and test Critical systems shall be capable of undergoing maintenance without interruption of critical services and shall be "fail-safe" while being maintained Design for easy removal, repair and replacement to the lowest level practical	Removal of hazard sources and operations Selection of least hazardous design or operations Safety factors, containment, isolation, purge, redundancy, backup systems, workarounds, safety devices, caution and warning devices, and procedures Maintainability program and adherence to maintenance and repair schedules	High Functions: station keeping, ECLSS, tracking, thermal control, routine operations Minimize crew and/or ground involvement in system operation Minimize routine tasks Functions: station keeping, ECLSS, tracking, thermal control	Minimize operations-driven costs and maximize effectiveness for users	Provide access to test points Support EVA test and checkout	Command and data handling system shall be capable of secure communications as required for normal and emergency operating conditions Secure voice/video communications shall be provided between crew and ground Payloads responsible for their own command and data encryption	Meet normal manned space flight standards	Initial hardware/software shall be capable of being replaced by or integrated with higher technology systems as they become available in areas anticipated to provided economical growth in capability	Hermetic seal
: 0.99999 s: TBD	Commonality and modularity to reduce costs and spares provisioning, optimize functional interfaces and software module allocation	Space-maintainable, long-life, low-maintenance hardware suitable for robotic removal and insertion, computerized verification test, common tooling, accessibility		High Functions: C/O, FD/FI, targeeng, rendezvous, and proximity operations	Design to cost Reusability reduces ratio of initial equipment cost to total operational cost Design for low-cost maintenance					
: 0.998 s: (30% ation)		BIT/IHM, power-down for repair MMTR 6 hrs		Semiautonomus Functions: station keeping, thermal control, minimize crew workload, unattended ~ 50% of time						
: 0.998 s: (30% ation)				Low Functions: systems monitoring, attitude hold (with manual override)						
: g s: TBD ution)		MTTR: 30 min internal, 6 hr external BIT/IHM, on-line (in-flight) and off-line (ground) spares		High Functions: GN&C, sequencing, systems monitoring, ECLSS, rendezvous and dock (with manual override)						Lunar dust, static charge encourages accumulation
, g s: TBD ution)		BIT/IHM, on-line (in-flight) spares, on-line and off-line repair MTTR: 30 min internal, 6 hr external		High Functions: GN&C, sequencing, systems monitoring, ECLSS, rendezvous and dock (with manual override), environmental analysis, thermal control						Finely ground windblown dust

C910976 11x17 B

Duration: 10 sec/flight in each of orbiter X_0, Y_0 and Z_0 axes. (The exposure duration of 10 sec/flight does not include a fatigue scatter factor. A fatigue scatter factor appropriate for the materials and method of construction is required and shall be not less than 4.0.)

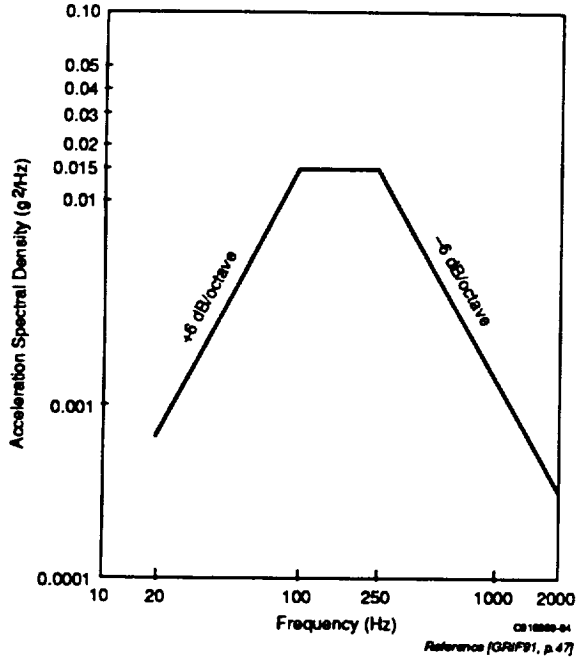


Figure 3-11. Shuttle Vibration Environment: Unloaded Main Longeron Trunion-Fitting Vibration

Duration: 14 sec/flight in each of orbiter X_0, Y_0 and Z_0 axes. (The exposure duration of 14 sec/flight does not include a fatigue scatter factor. A fatigue scatter factor appropriate for the materials and method of construction is required and shall be not less than 4.0.)

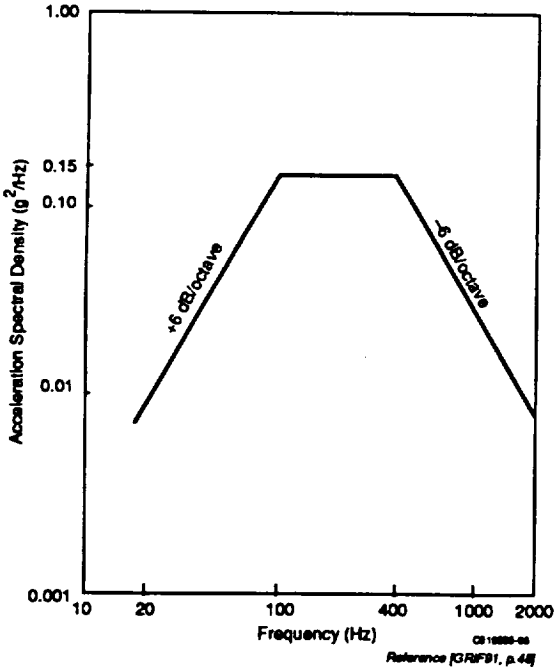


Figure 3-12. Shuttle Vibration Environment: Unloaded Keel Trunion Fitting Vibration

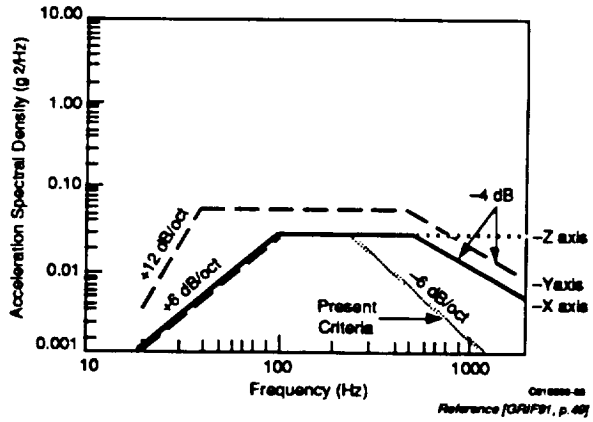


Figure 3-13. Shuttle Vibration Environment: Orbiter Main Longeron Random Vibration Criteria Derived from Flight Data

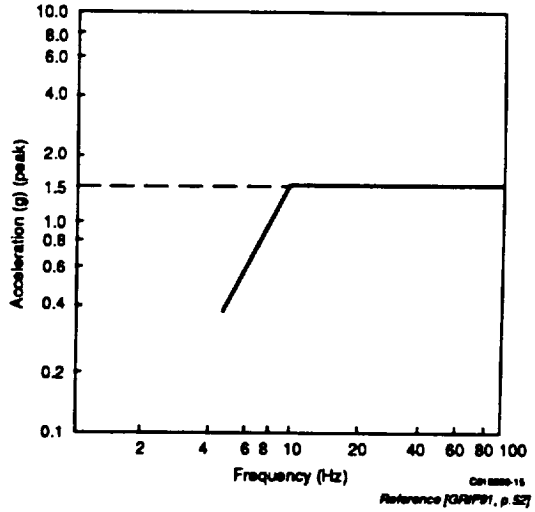


Figure 3-14. Ariane Vibration Environment: Longitudinal Sinusoidal Vibrations

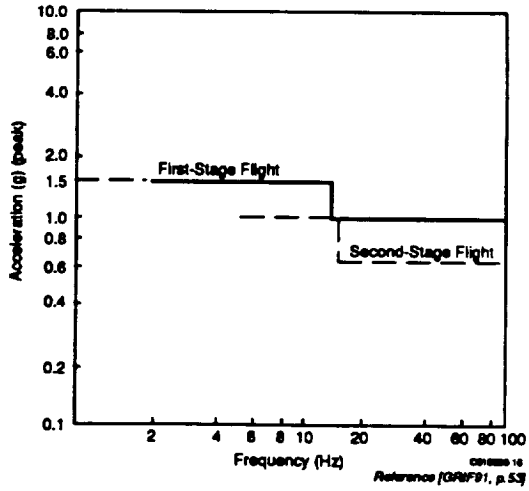


Figure 3-15. Ariane Vibration Environment: Lateral sinusoidal Vibrations

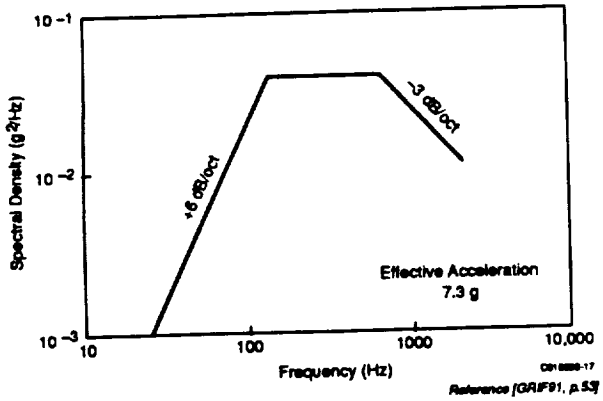
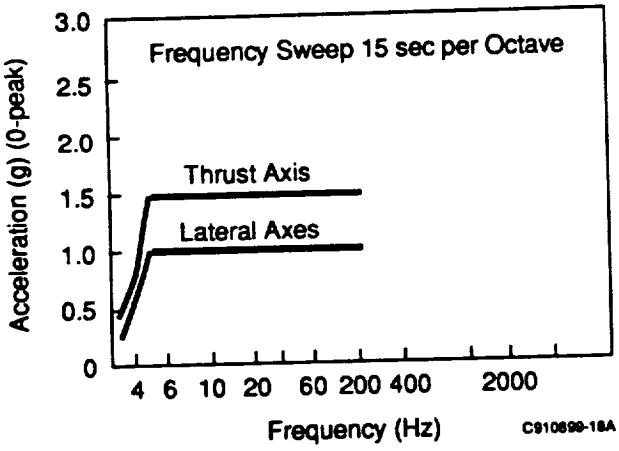
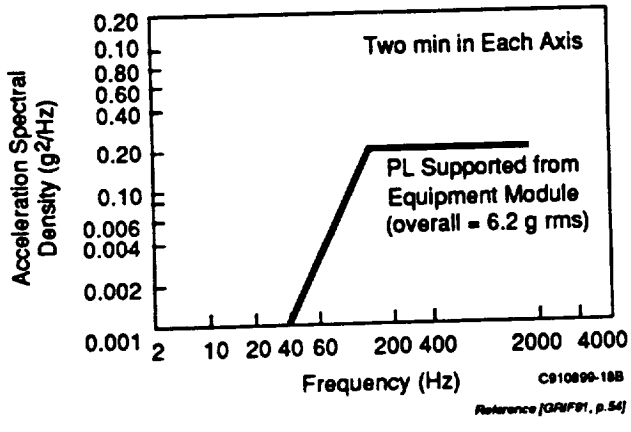


Figure 3-16. Ariane Vibration Environment: Random Vibrations



(a) Recommended Sinusoidal Vibration Environment



(b) Expected Random Vibration Spectrum

Figure 3-17. Atlas-Centaur Environment

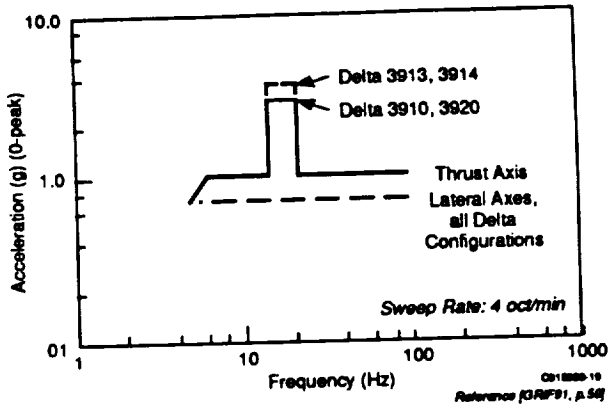


Figure 3-18. Delta Sinusoidal Vibration

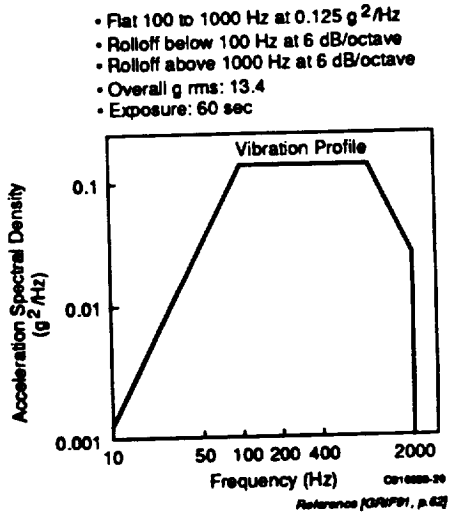


Figure 3-19. Titan 34D Vibration Environment: IUS/Spacecraft Interface Random Vibration

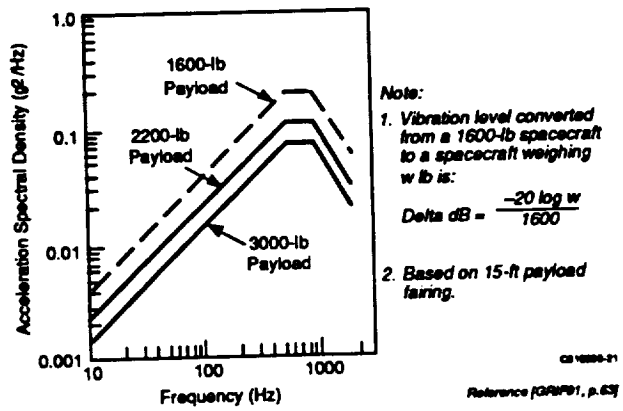


Figure 3-20. Titan 3C Vibration Environment: Transtage/ Spacecraft Interface Random Vibration

ETO Shock Environment—Spacecraft shock environments are associated with stage separations, pyrotechnics, docking, landing, and recovery. Figures 3-21 through 3-24 illustrate Delta and Titan launch vehicle shock data. Launch vehicle shock requirements are considered "High." Avionic shock environments can be as high as 10 g at landing to 1000 g at separation (location dependent). The shuttle avionics aft bay overall shock requirement is 20 g.

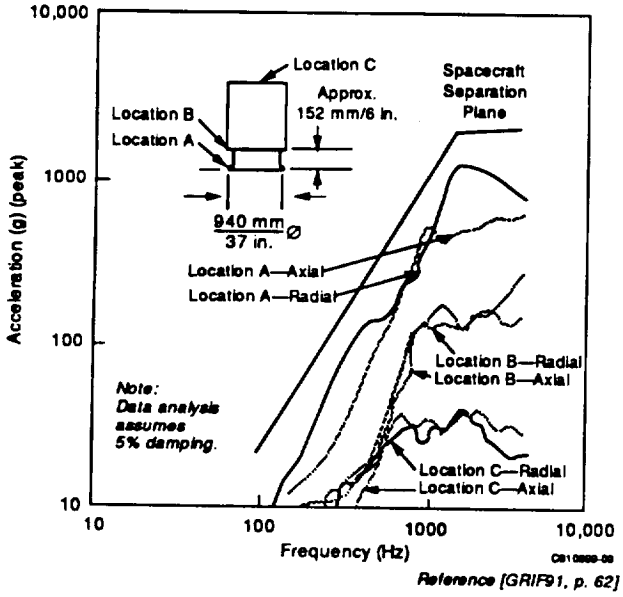


Figure 3-21. Delta Marman Clamp Shock Test Data

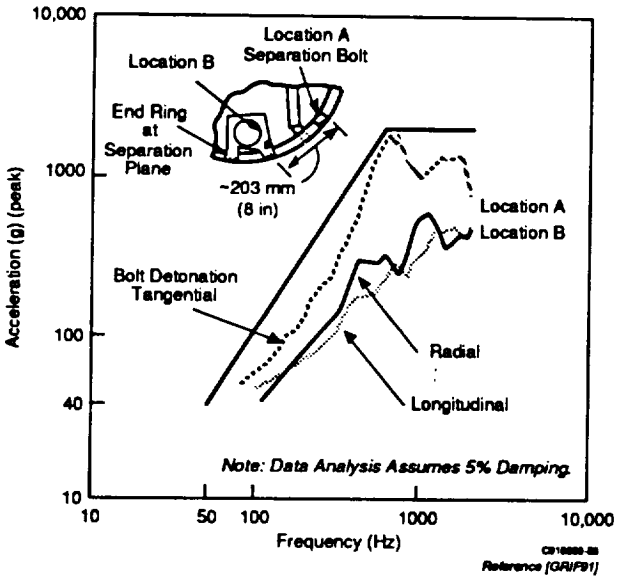


Figure 3-22. Delta Spacecraft Separation Shock Data (5414 Fitting)

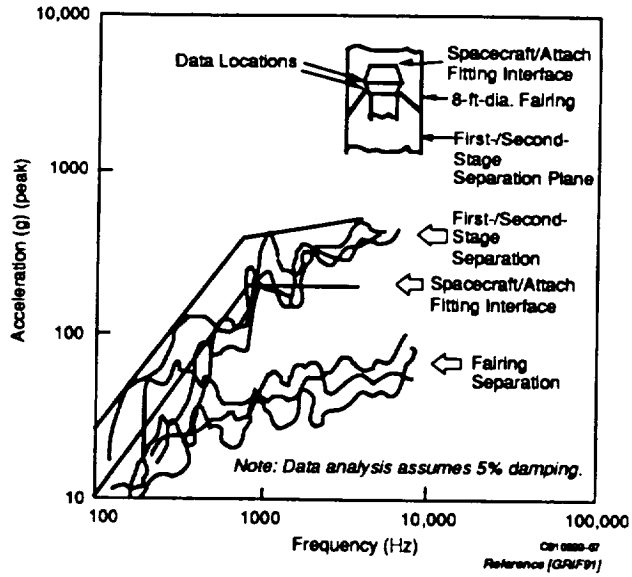


Figure 3-23. Delta "Straight-Eight" Ground Test Shock Separation Data

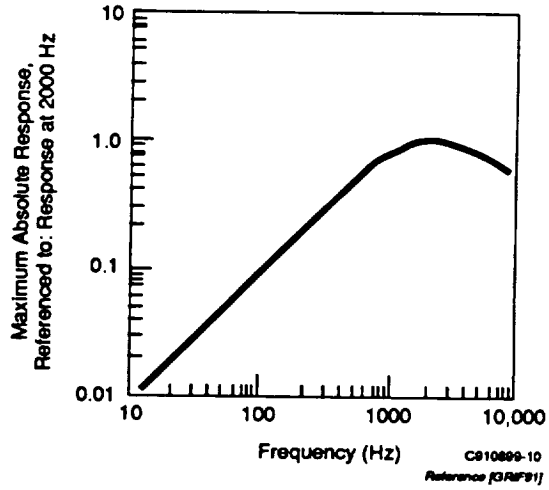


Figure 3-24. Titan 3C Shock Environment: Payload Fairing Shock at Spacecraft Interface, Normalized at 2000 Hz

COTS⁺ Capability—Commercial aircraft shock requirements are associated with handling (shipping container and bench handling drop tests) and crash safety. Although the equipment is not required to operate during the tests, the test articles will be inspected and operated at the conclusion of the tests and must show no failure, malfunction, or out-of-tolerance performance. Free-fall heights are up to 30 in., depending on the weight of the article.

COTS⁺ Shock Requirement—Definition of new ETO shock environment tests for COTS⁺ products is recommended and will be used in the COTS⁺ requirements base-

line. Shock tests at to-be-specified g levels will conform to shock requirements for aerospace equipment per MIL-E-5400T (i.e., 18 impact shocks consisting of three shocks in opposite directions along three mutually perpendicular axes). It will be a COTS+ baseline requirement to provide shock attenuation using physical structures, physical partitioning, and the distribution of Civil Market COTS products to locations where shock environments are within their operating envelopes.

ETO Temperature Environment—Various avionic space temperature environments were identified for the ETO mission:

- –186°C (–302°F) to 150°C (302°F) avionics [SPAC90];
- –46°C (–50°F) to 32°C (90°F) SSMEC operating [CONT73];
- –128°C (–200°F) to 94°C (200°F) SSMEC nonoperating [CONT73];
- –62°C (–80°F) to 65°C (149°F) STS avionics bay;
- –25°C (–13°F) to 65°C (149°F) avionics;
- –157°C (–250°F) to 121°C (250°F) STS cargo bay with doors open.

COTS+ Capability—Commercial aircraft avionics are designed to withstand operating temperature ranges from –15/–25°C to 65°C, depending on aircraft manufacturer specifications. The temperature may be either controlled or uncontrolled. Uncontrolled, passively heated, and cooled equipment will rely on radiation and natural convection from all sides of the equipment. No credit can be taken from heat conduction to equipment trays.

COTS+ Requirement—Since portions of the ETO mission are within a partial vacuum environment, uncontrolled COTS+ equipment will use radiative exchange from all six sides of the equipment and heat conduction to equipment trays, and will be accommodated by COTS+ requirements. If necessary, it will be a COTS+ baseline requirement to provide controlled thermal environments through physical partitioning and the distribution of Civil Market COTS products to locations where temperature environments are within their operating envelopes.

At launch, conductive thermal cooling will be provided from air convection, and thermal lag will be used to support heat transfer throughout the initial mission phase. An active thermal control system (ATCS) providing avionics bay heat rejection will be used for avionics required to be operational over longer durations. During checkout and prelaunch ground operations, heat rejection will be energized with ground power. From liftoff to approximately T+125 sec, thermal lag will be used. Flash evaporator operation subsequently commences and continues until vehicle radiators are deployed, as in the Shuttle mission.

COTS+ equipment operating temperature ranges will be from –15°C to 65°C. A cost assessment tradeoff study is recommended to assess the utility of this requirement for Olive Drab Commercial components, which are commercial products modified to withstand space requirements.

ETO Radiation Environment—The Van Allen inner and outer belts lie between approximately 0–1 and 2–3 earth radii, or between 0–4,000 and 8,000–12,000 miles above the surface of the earth, respectively. The ETO mission ends in LEO, which extends to approximately 621 miles (1000 km) above earth. The radiation belts protect the launch vehicle against solar flares by providing a highly effective shield.

Protection from total dose and dose rate transient effects can essentially be guaranteed with known and usually reasonable amounts of shielding in combination with careful use of radiation-hardened parts.

The radiation environments for LEO, geostationary, and an elliptical high-earth orbit (180 x 10,000 nmi) are shown in Figure 3-25, and Figure 3-26 shows the radiation environment for circular orbits. More high-energy protons are trapped in the inner Van Allen belt, and the effect of shielding attenuates the effects of low-energy electrons trapped in the outer Van Allen belt.

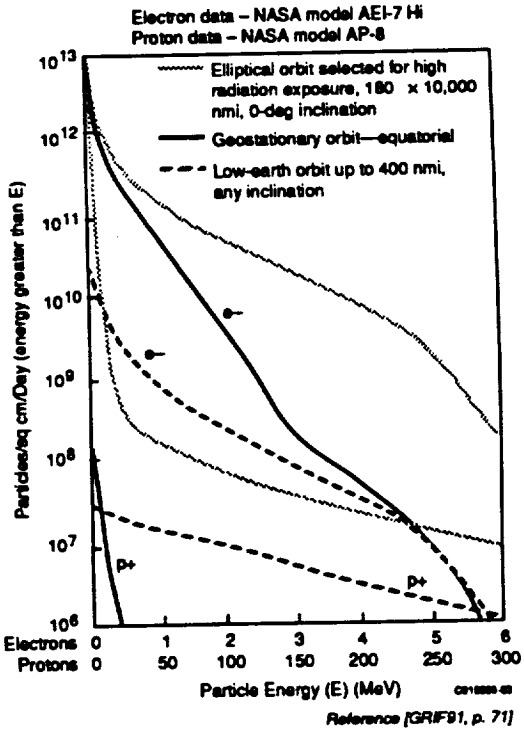


Figure 3-25. Natural Radiation Environment

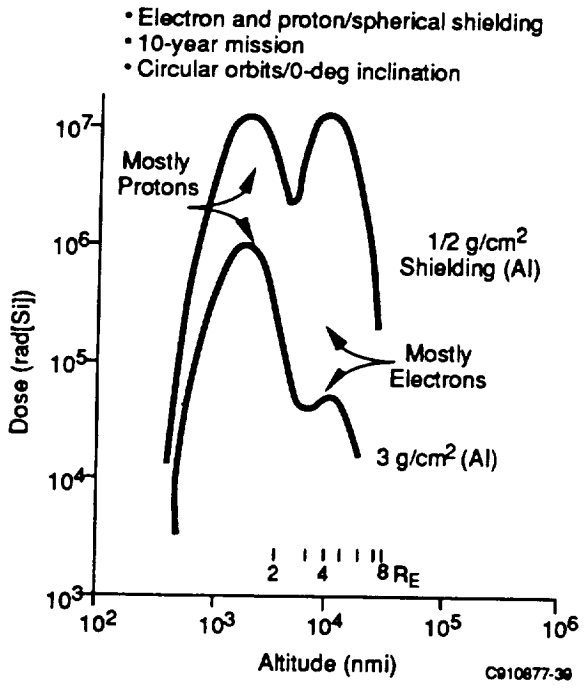


Figure 3-26. Radiation Environment for Circular Equatorial Orbits

COTS⁺ Requirement—The ETO radiation environment is considered "Medium." As a minimum, COTS⁺ equipment will be protected with shielding normally used against lighting strikes. In addition, the requirements will:

- Minimize susceptibility of electronic parts to single-event upsets (SEUs) by locating COTS⁺ electronics within radiation-shielded compartments.
- Assure SEU recovery and protection against latchup.
- Provide for the assessment of COTS⁺ radiation tolerance and possible substitution of more radiation-tolerant parts at the vendor's facility without significant additional recurring cost, e.g., pin-for-pin replacement of integrated circuits with epi-layer CMOS technology parts. Table 3-2 illustrates the radiation hardness levels for various semiconductor technologies.

ETO Partial Vacuum Environment [GRIF91]—The design of electronic equipment intended for use in launch vehicles is affected by gas ionization, as are spacecraft intended for operations in low-earth orbits. In a partial vacuum environment, low-density gases are easily ionized, providing excellent but unintended conductive paths between points in electronic hardware that are at moderate to high potential differences. This tendency is aggravated by the fact that at high altitude, the residual molecular and atomic species are already partly ionized by solar ultraviolet light and various collision processes.

Table 3-2. Radiation Hardness Levels for Semiconductor Devices

Technology	Total Dose, rads (Si)
CMOS (soft)	10^3–10^4
CMOS (hardened)	5×10^4–10^6
CMOS/SOS (soft)	10^3–10^4
CMOS/SOS (hardened)	$>10^5$
ECL	10^7
I^2L	10^5–4×10^6
Linear IC^2s	5×10^3–10^7
MNOS	10^3–10^5
MNOS (hardened)	5×10^5–10^6
NMOS	7×10^2–7×10^2
PMOS	4×10^3–10^5
TTL/STTL	$>10^4$

C910877-40

A key point is that if any equipment is to be energized during the launch ascent, care must be taken to prevent electrical arcing during certain phases of flight.

COTS⁺ Requirement—COTS⁺ equipment that may be powered on during the ascent phase will be operated during the evacuation phase of thermal vacuum chamber testing.

ETO Acoustic Environment—Titan IIS and MLV IRD acoustic environmental conditions are illustrated in Figures 3-27 through 3-29 and Table 3-3 provides maximum estimated noise levels for the Titan 34D/IUS.

SSMEC—The Space Shuttle main engine near-field acoustic environment is 174 dB.

COTS⁺ Capability—Commercial aircraft normally do not specify acoustic requirements.

COTS⁺ Acoustic Requirement—Per MIL-STD-810, equipment located in areas where noise levels are 130 dB or less do not require testing to noise environments. Acoustic qualification will be required for COTS⁺ equipment installed in high acoustic environments such as near engines.

3.2.3 Transfer Missions

The transfer mission will be to deliver vehicles, structures, components, fuel, supplies, and crew to high-altitude orbits or lunar/planetary orbits. Additional operations during intra-solar-system travel will be astronomical observations, training, and landing simulations.

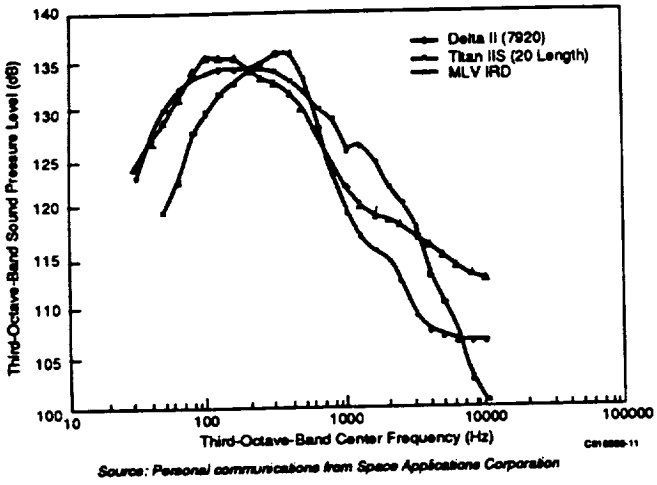


Figure 3-27. Fairing Internal Acoustic Environment

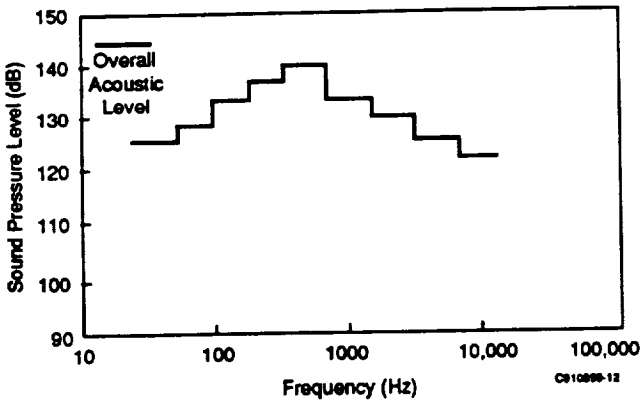


Figure 3-28. Delta Acoustic Environment

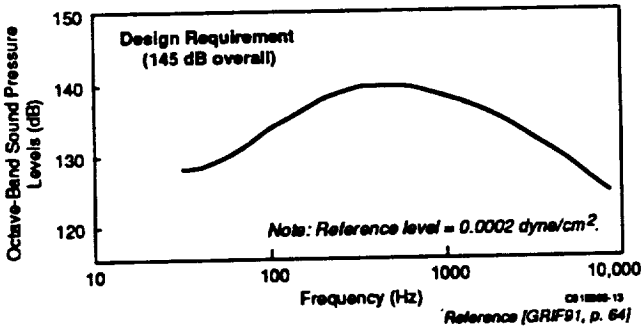


Figure 3-29. Titan 3C Payload Fairing Internal Acoustic Spectrum

3.2.3.1 Transfer Durations—Mars mission durations up to 1000 days have been projected. The mission would include 400 days for the round trip and a 600-day stay on Mars. However, the first trip would be shorter for several reasons.

Table 3-3. Envelope of Maximum Estimated Noise Levels Internal to Payload Fairing for Titan 34D/IUS Launch and Flight

Third-Octave-Band Center Frequency (Hz)	Third-Octave-Band Vibration (dB)
25	145
31.5	121
40	122.5
50	124
63	125.5
80	127
100	129
125	130.5
160	131.5
200	132.5
250	133.5
315	134
400	134.5
500	134.5
630	134
800	133.5
1000	133
1250	131
1250	131
1600	129.5
2000	128.5
2500	126.5
3150	125
4000	123
5000	121.5
6300	120
8000	118

Reference [GRIF91, p. 50]

Because psychological and physiological problems increase with trip time, the first trip may be limited to under 500 days. It also may not be feasible for a first mission to stay longer than 30 days on the surface because of launch windows, crew safety, and the lack of meaningful tasks to accomplish [UM-A91]. The University of Minnesota Task Team I Mars Integrated Transportation System (MITS) mission profile is as follows:

- Outbound, approximately 175 days using Venus flyby;
- Inbound, 249 days;
- Subtotal, 424 days;
- Stay time on Martian surface, 30 days;
- Total mission, 474 days.

The University of Minnesota Task Team II concept sends an unmanned Mars Habitation Module (MHM) to Mars autonomously prior to the manned mission with a Mars Excursion Vehicle (MEV) onboard the Mars Transfer Vehi-

cle (MTV). The MHM transfer time (using cryogenic boosters with low ISP) is approximately 500–600 days. This requires that the MHM be launched several years ahead of the manned mission [UM-B91].

3.2.3.2 Transfer Environments—Since all vehicles must endure the launch environment powered or unpowered, avionics for missions other than launch should meet environmental requirements unless more extreme environments (radiation, temperature, vibration) or effects (e.g., more heat generated by operating electronics) are evidenced.

Transfer Vibration Environment—Transfer vehicle vibration environments are considered "Medium" and not as harsh as the launch environment. However, the transfer vehicle avionics must endure launch vibration environments. Transfer vehicle avionics will be qualified to launch vibration requirements.

Transfer Acceleration Environment—Transfer vehicle acceleration environments are considered "Medium" and not as harsh as the launch environment. However, transfer vehicle avionics must endure launch accelerations. Transfer vehicle avionics will be qualified to launch acceleration requirements.

Transfer Shock Environment—Transfer vehicle shock environments are considered "Medium" and not as harsh as the launch environment. However, transfer vehicle avionics must endure launch shock environments; therefore transfer vehicle avionics will be qualified to the same levels as the launch shock requirements.

Transfer Temperature Environment—The transfer vehicles are exposed to direct sunlight (77°C) and darkness (–74°C). The vehicle will provide internal conduction paths and thermal control to accommodate ±150°C temperature differences between sunlit and dark sides. Heating rates for aerodynamic capture will be kept low. The maximum edge temperature of an aerobrake on earth aerocapture is approximately 600°C. Qualification of transfer vehicle avionics to launch vehicle temperature requirements with thermal control is sufficient for the transfer vehicle.

Transfer Radiation Environment—Spacecraft in transit above the Van Allen belts or in interplanetary space are exposed to solar-generated radiation and galactic cosmic rays. Although the dose levels from these sources have been said to be negligible, the total radiation environment enroute to Mars is more than 100 times greater than that encountered in a lunar mission.

The greatest radiation exposure threats are solar proton events and galactic cosmic radiation [NACH85]. Solar flares can produce severe single-event upset problems, since they consist of a large proportion of high-speed heavy nuclei particles against which it is impossible to shield [CUNN84 & CUNN85].

Major solar flares occurring in 11-year cycles, such as the August 1972 event, will require the equivalent of over 40 g/cm^2 aluminum shielding. A storm cellar wall or enclosure with the equivalent of 5.8 in. of aluminum must be provided to protect the crew for physiological purposes. The problem with aluminum is that as its thickness increases, secondary nuclear reactions produce more radiation than primary particles. However, Mars missions are planned for solar minimums and decrease the chance of solar flares.

A nuclear thermal reactor propulsive engine is used in the baseline vehicle design to provide higher ISPs, more acceleration for less propellant, lower cost, and a reduction in trip time. Shielding will be used to provide avionic and crew protection.

Transfer vehicle radiation environments are considered "High."

COTS$^+$ Radiation Requirement—COTS$^+$ avionics will require a protected environment, radiation-tolerant components, and recovery mechanisms from single-event upsets. Protection from total dose effects can essentially be guaranteed with known and usually reasonable amounts of shielding in combination with careful use of radiation-hardened parts. Figure 3-30 illustrates total doses for a deep-space mission and the effect of aluminum shielding for protecting avionics.

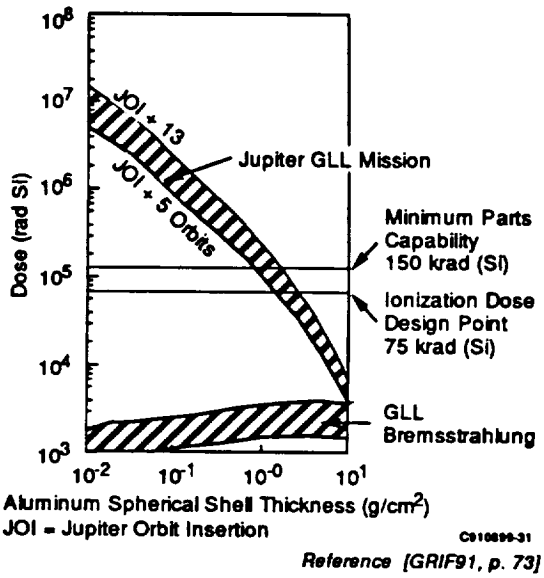


Figure 3-30. Electron Dose vs. Aluminum Shield Thickness for the Galileo Mission

A storm cell or equivalent will be provided to protect crew and critical avionics from major upsets. With a proper design, it may be possible to incorporate shielding for solar events with nuclear reactor shielding for the whole vehicle avionic suite, regardless of location.

Transfer Partial Vacuum Environment—

Material Outgassing [GRIF91]—Most materials will outgas to some extent in a vacuum environment. Metals will usually have an outer layer into which gases have been absorbed during their tenure on earth and which is easily released once in orbit. Polymers and other materials composed of volatile compounds may outgas extensively in a vacuum, losing a substantial fraction of their initial mass. Some basically nonvolatile materials, such as graphite-epoxy and its composites, are hygroscopic and absorb considerable water from the air. This water will be released over a period of time once the spacecraft is in orbit. In a vacuum, some plating materials, when warm, will migrate to cooler areas of the spacecraft, where they recondense; cadmium is notorious in this regard.

Outgassing materials can be a problem for several reasons. In polymeric or other volatile materials, the nature and extent of the outgassing can lead to serious changes in the basic material properties. Even where this does not occur, as in water outgassing material from graphite-epoxy, structural distortion will result. Such composites are often selected for applications where structural alignment is critical because of their high stiffness-to-weight ratio and low coefficient of thermal expansion.

Outgassing is a problem in that the vapor can recondense on optical or other surfaces and degrade device performance. Even if the vapor does not condense, it can interfere with certain delicate instruments. For example, ultraviolet astronomy is effectively impossible in the presence of even trace amounts of water vapor.

The COTS+ Requirement—COTS+ avionics will be qualified by analysis to ensure no detrimental outgassing effects.

3.2.4 Excursion Missions

The primary purpose of excursion missions will be to transport personnel and cargo between parking orbits and lunar or Mars surfaces.

3.2.4.1 Excursion Durations—Projected lunar and Mars excursion durations are:

- Lunar—On orbit four days per mission, one to two missions per year, and five missions per lifetime.
- Mars—Six days for a nominal mission and 30 days for contingency planning; 800 days possible lifetime (200-day transit, 600 days on surface and return to Mars orbit to rendezvous with the MTV, and abandoned).

3.2.4.2 Excursion Environments—Excursion vehicle environmental requirements are cited in the following paragraphs. No excursion environments or operations requiring additional concern are noted when compared to launch and transfer vehicle environments. Launch or transfer vehicle environmental requirements are specified where applicable.

Excursion Vibration Environment—Excursion vehicle vibration environments are considered "Medium" and not as harsh as the launch environment. However, excursion vehicles must endure launch vibration environments; therefore, excursion vehicle avionics will be qualified to launch vibration requirements.

Excursion Acceleration Environment—Excursion vehicle acceleration environments are considered "Medium" and not as harsh as the launch environment. However, excursion vehicles must endure launch acceleration environments; therefore, excursion vehicle avionics will be qualified to launch acceleration requirements.

Excursion Shock Environment—Excursion vehicle shock environments are considered "Medium" and not as harsh as the launch environment. However, excursion vehicles must endure launch shock environments; therefore, excursion vehicle avionics will be qualified to launch shock requirements.

Excursion Temperature Environment [SPAC90]—The Martian surface temperature varies from –125°C to 25°C and the vehicle must accommodate ±150°C.

The lunar excursion vehicle must accommodate –180°C to 150°C. Shadowed lunar craters at the poles have surface temperatures of –233°C. At the Apollo 17 site, day to night temperatures ranged from –117°C to 110°C.

Qualification of excursion vehicle avionics to launch vehicle temperature requirements with thermal control is sufficient for the transfer vehicle.

Excursion Radiation Environment—Excursion vehicle radiation environments are considered "Medium" for lunar and "High" for Mars excursion vehicles. The crew and avionics will be provided adequate shielding onboard the vehicle. Protection from solar flare radiation levels will be provided for avionics required for rendezvous. This pro-

tection will be a storm cell or equivalent to protect operating and/or nonoperating critical avionics from permanent damage. Crew protection during anticipated solar flares will be entry into the transfer vehicle and/or surface modules after solar flare warnings.

3.2.5 Orbital and Surface Missions

Orbital and surface system operations include space experiments, astronomy, exploration, geologic sampling, and construction.

3.2.5.1 Orbital and Surface Durations—The SSF mission is 30 years on orbit. A lunar spaceport lifetime may be beyond 20 years. The Mars habitat module may be occupied for up to two years and have a lifetime up to 20 years.

3.2.5.2 Orbital and Surface Environments—Since all vehicles must endure the launch environment powered or unpowered, avionics for missions other than launch should meet environmental requirements unless more extreme environments (radiation, temperature, vibration) or effects (e.g., more heat generated by operating electronics) are evidenced.

Orbital and Surface Temperature Environment—The lunar spaceport must operate within a lunar temperature range from –180°C to 120°C.

Orbital and Surface Radiation Environment—A permanent platform may encounter radiation doses up to 3000 Mrad, and lunar and Martian surface stations/modules may accumulate comparable amounts. NASA has set a 50 rad requirement for SSF.

Protection from solar winds, galactic cosmic radiation (GCR) sources, and solar particle events (SPEs) from solar flares will be provided for operating and nonoperating critical avionics. This protection will be a storm cell, safe, or equivalent structure to protect critical avionics from permanent damage.

COTS+ Requirements—Orbital and surface vibration, acceleration, shock, acoustic, and temperature requirements will be as specified for launch vehicles, and radiation protection will be provided by incorporating sheltered avionic bays, safes for avionic cold spares, and/or storm shelters.

3.3 Verification and Validation Issues

3.3.1 Introduction

This subsection provides guidelines for the verification and validation (V&V) of COTS+ integrated modular avionics and is based on the principles presented in ARINC Project Paper 651 for certifying IMA in commercial air transport category aircraft. It provides background information and airline philosophy on the certification process, which may be incorporated within COTS+ applications. It contains recommendations that are expected to minimize the effort necessary to certify new avionic systems and modified avionics equipment subject to certification.

Commercial certification provides guidelines for the implementation of V&V procedures for COTS+ avionics. Commercial certification regulations and procedures are analogous to Department of Defense (DoD) validation specifications and tests; both ensure safety of operations. Included within the certification definition are the procedures used to verify that designs meet specified requirements.

3.3.2 Airline Philosophy

Philosophically, airplane certification demonstrates that a specific aircraft function is within acceptable safety limits. It demonstrates a degree of confidence in the performance and operation of a system. It is not meant to be a set of activities designed solely to meet the regulations. Rather, it sets the level of acceptable safety for a new system or, in the case of modifications, demonstrates that existing overall safety is not degraded.

To aid in this process, national regulatory authorities have established sets of regulations and other advisory documents that build on past experience. Therefore, certification is to be a living, flexible process capable of absorbing the developments in aviation and associated technology while still maintaining its purpose—the safe aircraft.

Documents supporting the certification plan ideally contain only text, drawings, and data that are relevant to the certification. More documentation is not necessary to ensure successful certification and may overcomplicate and delay the process. The end result of certification is approval of a function in the aircraft (and ultimately the total aircraft), but, as part of the certification process, certain steps of certification are defined and may be accomplished independently.

3.3.3 Responsibility for Certification

Ultimately, it is the responsibility of the users to ensure that their vehicles are safe. Although a regulatory agency has ultimate responsibility for aircraft certification, it may delegate that responsibility to an applicant who has demonstrated competence in the certification process. The regulatory agency should assess the experience and resources of each applicant to determine if the applicant's certification plan is sound.

Manufacturers are responsible for type certification of the vehicle. They ensure that vehicles supplied to the users meet all of the pertinent regulations. Users often contract with the manufacturers to perform supplemental type certification (STC) after the vehicle is in service.

3.3.4 Verification and Validation of COTS+ IMA

In the COTS+ IMA concept, general-purpose computers execute a variety of application programs within a standardized software environment. With this approach, individual avionics functions shed their LRU identity common with previous generations of equipment. Resources are shared, and communication is performed in a more highly integrated manner than was possible with independent LRUs. This level of integration results in the potential for undesirable interrelationships between separate avionic functions. The validation task to demonstrate acceptable aircraft safety is different for IMA and LRU equipment.

Verification and validation tasks are composed of three distinct efforts:

- Confirmation of the general environment provided by the cabinet,
- Confirmation of the operational behavior of each function intended to reside in a cabinet,
- Confirmation of the resultant composite of functions within a specific cabinet.

All of these concepts are present in LRU validation but not as separate identifiable tasks. The COTS+ IMA validation process shall optimize each of these areas separately.

3.3.4.1 Cabinet Environment V&V—A COTS+ cabinet provides all of the physical and computational resources necessary for the various avionic functions to be reduced to just a software program. This is essentially all the hardware, e.g., the mechanical racking and enclosure, power conversion and distribution, backplane bus, and computer. The computer consists of the CPU, program store memory, scratchpad memory, timing and control circuitry, internal data paths, port to backplane bus, and executive (operating system) software.

Cabinet Hardware Resources—Each facet of the cabinet hardware is implemented with a strategy for fault tolerance. These strategies include both redundancy and design margin. Redundancy provides the ability for continued operation in the event of a random component failure, and design margin provides the ability for continued operation at extreme stress levels.

V&V of the hardware aspects of the cabinet environment ensures that the cabinet components provide their respective functions with the intended fault tolerance over the entire anticipated environmental spectrum. The environmental spectrum includes temperature, vibration, and EMI primary power transients. Verification at this level concentrates on electrical characteristics: waveforms, voltage and current levels, monitor detection thresholds, resource allocation circuits, and the like.

Executive Software Program Resources—The executive software program provides task scheduling, resource management, and supervision of the operational application software programs and is implemented with a strategy for fault tolerance. This strategy includes memory management, computational timing budgets, and monitoring the execution of the application programs for possible violations. Reconfiguration and recovery methods are to be provided for each potential violation.

Verification of the software aspects of the cabinet environment ensures that the cabinet executive provides its intended function. The operation of the executive shall be verified to conform to the requirements and the structure of the implementation.

3.3.4.2 Avionic Function Operational Verification—Each avionic function may consist of several software application programs executed by one or more computers. The various functions are independent and isolated from one another. Any intended interaction between functions occurs as an overt use of system resources. A particular function most likely will be composed of several constituent pieces, convenient to its particular needs.

The constituent pieces or tasks contain the implementation of the operation of the specific avionic function. This includes interfaces to other functions, data conditioning, sensor source selection, crew interface, computational algorithms, fault monitoring, and so on.

Function operational verification ensures that each specific application program performs as intended by confirming the accuracy and adequacy of performance over the range of input data conditions, mode transitions, and flight scenarios. This process includes module testing, integration testing, functional testing, and other tests. Verification at this level concentrates on confirming the presence of intended function, requirements mapping, operational performance, and test coverage.

Each integrated function should be individually verified as part of the IMA cabinet. Robust partitioning concepts are necessary to ensure that once a function is verified, it can remain

hosted in a cabinet containing any combination of uncertified functions without jeopardizing the status of any verified functions. Composite cabinet verification (simultaneous verification of all IMA functions) is not necessary nor required.

3.3.4.3 Validation of Degraded Modes of Operation—One of the main drivers for COTS+ IMA is avionic function availability. Fault detection, isolation, and the use of redundant components are necessary to fulfill these needs.

A principal benefit of COTS+ IMA is the ability to exploit the inherent fault tolerance of the system to allow users to defer maintenance actions. This can be accomplished by designing equipment to perform with degraded modes of operation. Although airlines use a scheduled maintenance concept, the extent to which it is used and the criticality of functions involved renders this concept different in the COTS+ IMA deferred maintenance concept.

With COTS+ IMA and the availability of shared resources, it is possible to achieve higher levels of fault tolerance for a greater number of systems and for systems of lower criticality. This allows a large number of systems to be certified for fail-operative or degraded modes of operation.

In the most forward-looking approach to IMA, the COTS+ IMA system has the responsibility to detect and isolate all failure conditions, enable redundant components, inhibit actions by failed components, and determine whether flight or ground crew need to be notified. It will also determine if operating restrictions apply.

Some of the validation issues include the following:

- The failure modes and effects of the avionics need to be rigorously examined in a fully operational state and in degraded modes of operation.
- The effectiveness of built-in-test algorithms to correctly identify failures and reconfigure the system around those failures will be as critical as the system itself.
- Issues of crew awareness and reliance on the system to enforce operational restrictions shift from vehicle operational procedure validation to validation of the degraded modes of operation.

It is expected that the transition to the deferred maintenance, degraded mode of operation concepts will be evolutionary and will progress as confidence is gained in IMA.

3.3.5 Configuration Control

The assurance of continuous dependability throughout the life of the vehicle is essential. To accomplish this, an acceptable system should be in place to ensure that the validated configuration is maintained. Configuration control is the means whereby it is determined that replacement items installed on the vehicle are acceptable in form, fit, and function and meet the legal and technical definition of being validated for their intended use. Each vehicle incorporates electronic documentation describing equipment installed thereon, including manufacturers' part and serial number.

3.3.5.1 Configuration Status—Throughout the production run of a vehicle design, changes and improvements will be made constantly. Improvements to engines, additional systems, and extended performance of existing systems can be expected. For example, extending the autoland performance of the flyback booster's guidance system into ILS CAT 111 conditions may require more attention and control than the installation of a radio altimeter. Retrofit of a performance management system on a fleet of vehicles may require certain features of a distance measuring equipment (DME) interrogator that not all of the previously interchangeable DMEs have.

Of great value to the users is the ability to use the same component across several fleets of vehicles. The configuration control system will be able to identify clearly any unique features of the fleet that might be affected by modification status or manufacturers' variables between similar equipment. Sometimes a new version of existing equipment is backward integratable on earlier vehicles, but the users' inventory of spares cannot be used on the later version airplanes. This type of one-way interchangeability is rarely of any use other than the potential it offers for modification of all existing inventory to the latest version.

3.3.5.2 Use of Manufacturer Parts List—The parts list applicable to a particular series of vehicle will include alternate parts that have been determined to be acceptable. This list may include interchangeable components specified by an ARINC characteristic supplied by different manufacturers. While this type of documentation has proved to be of significant economic benefit to the airlines, it introduces to the COTS+ concept the problems of identification, change control, and modification status accountability necessary in a configuration control system.

3.3.6 Software Changes

In the COTS+ IMA concept, support personnel use an onboard data loader to update software in equipment resident on the vehicle. The data-loading process will be described in modification documentation and/or LRU installation procedures, depending on the reason for the change. The transfer medium will provide the data in a standardized form.

The integrator and the onboard software loading system are responsible for ensuring the integrity of each software modification. An update might make minor changes to a single function without affecting the memory map or timing structure of the cabinet. An update might also make large reassignments of both resources. Both extremes should satisfy the consistency checks described earlier. To ensure correctness, these checks should be compared with known, required states of the system following the modification.

Users with the proper level of technical expertise may assume complete responsibility for one or more avionics cabinets. Functions may be reassigned, changes may be incorporated or initiated, and new applications that are specific to the user may be developed. In such instances, the user would accept the responsibility for verification and validation.

3.4 Maintainability and Testability

3.4.1 General

The benefits of dependability and cost are two key motivators toward incorporating a COTS+ maintainability and testability philosophy. The following paragraphs summarize these benefit.

3.4.1.1 Dependability—Deep-space extended-duration missions have been said to require avionic dependability better than fail-operative (FO) 10-failure probability, meaning that the avionics are fully operational after 10 like failures. The ramifications of this requirement are significant. Assuming that channel redundancy is implemented, 12 avionic channels would be required. Considerable effort would be required to implement such an ultra-high-reliable avionic system in a cost-effective (low-cost, high-utility) manner. The electronic design, redundancy management, and V&V for the system would require appreciable efforts.

Flight safety and maintenance benefits, however, are realized with the high-dependability requirement. The mean time before maintenance alert (MTBMA) will be several times the MTBF of a single channel. Improvement in system unreliability is achieved, and depending on single-channel failure rates, an order of unreliability improvement can also be achieved.

This subsection provides analysis applicable to the incorporation of COTS+ components in a quad-channel configuration in lieu of a 12-channel implementation implied by the desire to achieve 10-FO fault tolerance dependability. The concept uses a deferred maintenance philosophy to effect a lower cost, weight, and power configuration that can be designed and implemented with current expertise.

The deferred maintenance or fly-without-repair concept is also applied to expendable boosters in the strawman COTS+ maintenance concept presented herein. Although the deferred maintenance concept was not considered cost-effective within MPRAS Point Designs, it is to be reconsidered here because of COTS+ component cost utility and opportunity costs.

3.4.1.2 Cost—Two distinct cost benefits derive from the use of COTS+ technology within a COTS+ philosophy: (1) reduction of missed opportunity costs and (2) reduced maintenance support costs. Opportunity cost benefits are the result of incorporating a deferred maintenance concept. Reduced maintenance support cost benefits result from implementing new COTS+ IHM maintenance strategies and reduced maintenance support costs.

Opportunity Costs—Opportunity costs are viewed as the additional costs incurred whenever an event or opportunity is delayed and rescheduled to a later time; a delayed launch due to a component failure is an example. Another, perhaps more costly, example is if an avionic failure occurs enroute during a deep excursion mission and the end mission segment is scrubbed or postponed to another mission, resulting in the space vehicle's loss or return to earth—primary mission unaccomplished.

Maintenance Support Costs—Motivation toward the incorporation of COTS+ also exists because of cost benefits that can be achieved in long-term maintenance and support. To achieve these benefits, a COTS+ maintenance and testing strategy must be followed.

This subsection provides design guidance for developing a maintenance strategy for COTS+ IMA-equipped vehicles. It includes guidelines for the maintenance community on testing COTS+ IMA equipment. It focuses on specific recommendations concerning the testability and maintainability of IMA components. It discusses real-time reporting of COTS+ IMA faults and the storing of data representing COTS+ IMA faults. An interactive maintenance function is described that identifies, confirms, and isolates faults. Actions taken to correct faults and the verification of the results of such actions are also discussed in this section.

3.4.1.3 Deferred Maintenance—A COTS+ deferred maintenance concept will be used for all avionic subsystems using COTS+ components unless it is shown by analysis (noted under recommendations for further study) that this is not cost-effective. Analysis will include missed opportunity costs, including the costs of all supporting functions/organizations for the duration of launch recycles, postponements due to missing orbital-celestial launch windows, and postponements awaiting favorable weather conditions. The deferred maintenance concept is herein

earmarked for use within expendable launch vehicles and extended-duration transfer/excursion vehicles because of COTS+ cost advantages. It is recommended that the concept be evaluated for effectiveness in other client subsystems.

Expendable Boosters—A quad-redundant fly-without-repair architecture and maintenance philosophy is hereby recommended for implementation in COTS+ baseline expendable boosters for the following reason. Preliminary analysis indicates that implementing a COTS+ deferred maintenance concept costs less than $90K per ALS mission ($88.8K vs. $893K per ALS mission with space-qualified components) [MPRAS TM1]. The cost delta compares deferred maintenance implementation only to maintenance costs. It is believed that an assessment of opportunity costs, payload, and catastrophic losses will favor a COTS+ deferred maintenance concept. Table 3-4 shows the difference between using COTS+ components and space-qualified components when comparing deferred maintenance costs vs. maintenance costs for the 347 mission ALS reference vehicle. COTS+ costs were assumed to be one-tenth of custom space-qualified component costs. Five sets of avionic single-string MTBFs were used per the MPRAS study for parametric quantification of costs. The table shows triple modular redundancy (TMR) MTBFs for single-channel MTBFs of 200, 600, 2000, 6000, and 20,000 hours per MPRAS Technical Memo - 1 (TM-1). The table shows a much lower deferred maintenance cost delta for lower reliability systems (e.g., $34K for a TMR of 66.7 hours).

Table 3-4. Deferred Maintenance Delta Costs

TMR MTBF (hr)	Technology	Data Costs per Mission	Program Delta
66.7	MPRAS	$838.0K	$291.0M
	COTS+	$34.0K	$11.9M
200.0	MPRAS	$873.0K	$303.0M
	COTS+	$70.0K	$24.3M
667.0	MPRAS	$887.0K	$308.0M
	COTS+	$83.3K	$28.9M
2000.0	MPRAS	$890.0K	$309.0M
	COTS+	$87.3K	$30.3M
6670.0	MPRAS	$893.0K	$310.0M
	COTS+	$88.8K	$30.8M

Extended Missions—A maintained COTS+ quad-channel avionic baseline architecture shall be used in lieu of n-parallel channels to provide the 10-FO desired goal for deep-space, LTV/MTV, and excursion vehicles. By manually replacing failed components of a quad-channel system, the architecture can provide 10-FO dependability. Although mathematical models and formulas show improvement in availability using multiple components with a given reliability, there is a definite limit on the benefit to be gained by adding redundant elements. The utility of the concept is sensitive to avionic reliability and equipment on-time because of the extremely long flight duration of the MTV. Avionics may be energized for thousands of hours.

Assuming 200 days for transit, 600 days for Mars surface activities, and 200 days for return, 1000 days or 24,000 hours of avionic flight time is accrued. Avionic reliability, comprising inverse exponential functions, suffers immensely for mission times in the thousands of hours compared to 1- to 2-hour missions. Unless future manned mission single-string avionic reliability is fairly high, parallel redundancy provides minimal improvement.

To circumvent this problem, avionic equipment may be turned off for extended periods and/or higher reliability components may be used. The latter suggests Class S parts instead of Class B or commercial parts; this alternative does not fit within the COTS+ concept. The avionics may be de-energized for periods of time enroute and during surface visitations, thereby reducing the maximum 24,000-hour avionic on-time by a factor of three to 7,500 hours—which does not help much.

The COTS+ philosophy will be to implement a quad-channel architecture to reduce cost and complexity. A deferred maintenance concept will be instituted using cold spare COTS+ components to replace failed redundant elements and using storage cabinets to protect cold spares. Advantages of the COTS+ concept include module longevity derived from unpowered components, reduced power consumption, protection from galactic and solar radiation, and weight/volume savings from the elimination of chassis, backplane, and cable interfaces required for higher order redundancy.

A maintained system COTS+ concept will offer considerable reliability improvement for the LTV/MTV and excursion vehicles over unmaintained systems. Preliminary COTS+ assessments indicate system safety and spares count within goals. Further study of COTS+ reliability and maintainability is recommended to assess this concept, establish baseline channel reliabilities, and establish achievable spares requirements.

3.4.2 Centralized Maintenance Concept

COTS+ shall implement a centralized maintenance function for all spacecraft avionics. The function shall provide fault detection, fault isolation, and fault containment and allow faults to be positively identified before they are allowed to propagate to serviceable components. A central maintenance computer (CMC) providing these functions is incorporated within the Boeing 777 airplane's AIMS and is described in Appendix A. The CMC is defined within the COTS+ strawman architecture herein.

Avionics functions shall be designed to report their status, performance details, and faults during operation of the spacecraft (i.e., the flight mode). This assists maintenance personnel in scheduling maintenance actions before the deferred maintenance is performed.

The COTS+ maintenance concept is based on the application of fault tolerance techniques to an entire avionics system. Fault tolerance is to be applied to the entire avionics system from the sensors through the interfaces, to the processing, and ultimately to the display devices. The various methods for achieving fault tolerance are described in Subsection 4.5.

The details of the central maintenance concept are documented in ARINC Report 624, "Onboard Maintenance System."

3.4.2.1 Failure Data Recording—A method of recording fault information automatically should be part of the system design. Dedicated nonvolatile memory should be used to record all fault data. The capacity of the memory should be sufficient to store failure events that could accumulate in a 10-day period of 240 flight hours. This data shall be downlinked to earth for extended-duration operation (EDO) to clear accumulated data. Redundant storage of fault records is recommended to ensure that the data is available in the event of a storage medium failure.

The CMC cabinet should also contain nonvolatile memory to record all cabinet and related module faults. A section of memory should be dedicated to each cabinet to ensure fault data recovery, even in the event of total system failure.

At the module level, nonvolatile memory will be provided to record the module faults and the status of remaining levels of redundancy. A section of memory will be dedicated to each module to ensure failure data recovery in the event of total system failure.

3.4.2.2 Operational Reporting—There will be displays on the flight deck that can be used by the flight crew to determine the operational status of selected avionics equipment.

Annunciation—The flight crew should be automatically notified when a fault or accumulation of faults has impaired system performance to the extent where operational restriction or crew intervention is required.

Interrogative Annunciation—A method will be provided for the flight crew to interrogate avionics functions that affect flight operations. This function will annunciate the remaining levels of redundancy for each component. This will assist the flight crew in the preparation of maintenance actions prior to the deferred maintenance actions.

3.4.2.3 Maintenance Reporting—An avionics function will report its operating status to the central maintenance computer. In the case of a fully fault-tolerant avionics suite, a maintenance alert annunciation will automatically occur after a fault to indicate that corrective action may be necessary.

Real-Time Fault Reporting—Provision for real-time fault reporting is part of the COTS+ maintenance concept. The occurrence of a fault and the associated level of fault tolerance should be reported to the central maintenance computer and stored on the aircraft. The improved diagnostic capability afforded by a COTS+ architecture allows the flight crew to downlink fault data likely to result in maintenance assessments to the support maintenance center via data link. Designers should consider this option in their designs.

Ground-Based Downloading—The status of an avionics function should be downloadable via VHF data link or gate link by the launch support ground crew while the spacecraft is on the ground.

3.4.3 Onboard Maintenance Equipment

3.4.3.1 Central Maintenance Computer—The central maintenance computer is a key component in the COTS+ maintenance strategy. The central maintenance computer will conform to the recommendations of ARINC Report 624, "Onboard Maintenance System (OMS)."

3.4.3.2 Electronic Library—A database of maintenance information is to be used with the COTS+ concept. An electronic library system (ELS) of maintenance records, schematic diagrams, and troubleshooting tools is to be stored on manned vehicles. This will extend the ability for the spacecraft to be serviceable when it is away from ground maintenance stations. Uploading of databases will be provided via communication links while the vehicles are in transit or stationed at their lunar or Mars destinations. The ELS should conform to recommendations (TBD) similar to ARINC Report 649, "ELS."

3.4.3.3 Maintenance Access Terminal—A maintenance access terminal (MAT) should be placed in a location convenient to maintenance personnel. This terminal should enable maintenance personnel to perform BITE on the individual IMA cabinets, sensors, actuators, etc., and should include interactive tests where appropriate. It should also allow the operator to read maintenance memory and determine the current integrity level of IMA components.

The details of the MAT are documented in ARINC Report 624, "Onboard Maintenance System."

3.4.3.4 Onboard Printer—COTS+ status information should be available on hardcopy printout. A standard multifunction printer should be used for this function and should conform to ARINC Characteristic 744A, Full-Format Printer.

3.4.4 Interactive Maintenance Mode Function

In addition to passive reporting of faults and remaining redundancy levels, avionic functions should provide an interactive mode that can be accessed by authorized personnel. This mode can assist the ground crew in the identification or confirmation of a fault condition and the isolation of the fault to a single LRM. It should be possible to interrogate avionic functions and access failure data located in read-only memory while the aircraft is in flight. One method of accomplishing this is via data link.

3.4.4.1 Functional Testing—Each avionic function should be able to be individually ground tested through a functional test capability. Functional testing is defined as the complete testing of hardware and flight software in the operational mode. Such tests may be initiated by the maintenance crew and are performed by BITE within the various system components. Some functional tests can be initiated through the maintenance access terminal with no test equipment attached to the system. Functional testing may be used as a vehicle for verifying system safety after maintenance repairs.

Spacecraft System Level—Functional testing at the spacecraft level will be possible whereby the serviceability of the system as a whole is confirmed. In every case, there should be a high level of assurance that all components of a system are functional following a satisfactory test. Onboard maintenance systems are to be used to debug aircraft system wiring and confirm the integrity of the interfaces.

3.4.4.2 Hardware Testing—The ability to test hardware will be provided. Testing of specific hardware may be performed when functional testing detects a failure but is unable to detect its source. Generally, hardware is tested with the spacecraft in its normal configuration; however, special test software may be required to be downloaded into an LRM and special test equipment may be attached.

Spacecraft System Level—The spacecraft system tests will support spacecraft-level testing of all hardware functions.

Cabinet Level—Cabinet assemblies should be designed such that any individual cabinet may be tested independent of the total avionics system. A test access connection should be provided to interface test equipment such as a maintenance access terminal.

Module Level—All modules should be designed to support testing of hardware functions. This function includes the optional downloading of test software into the module from external test equipment.

3.4.5 Corrective Action Function

Corrective actions include those actions necessary to restore system and/or LRM operation such that the redundancy levels are present. Corrective actions can also involve the updating of component software.

3.4.5.1 On Spacecraft—COTS+ components will be designed to minimize the mean time to repair (MTTR). This includes both the removal and replacement of hardware components and the loading of new software.

Hardware—COTS+ components will be designed to allow the removal and replacement of all hardware components using hand tools. Spacecraft cable assemblies should be able to be disconnected from both ends. All LRMs and LRUs should be easily removable from the spacecraft.

Software—It should be a simple process to load new software into appropriate COTS+ components using an onboard data loader, maintenance access terminal, or data link. Protection should be provided to preclude actions by unauthorized personnel. Safety measures should be part of the loading procedure to ensure a successful load.

3.4.5.2 At Maintenance Stations—

Automatic Test Equipment—Automatic test equipment (ATE) will enable surface support maintenance centers to verify the proper operation of LRMs and perform troubleshooting. Such equipment will provide the capability to perform tests and download/translate BIT status data stored in memory. The ATE will conform to ARINC Specification 608A, "Design Guidance for Avionics Test Equipment."

LRMs will be designed with an ample number of clearly labeled test points to aid in troubleshooting. They will be designed to simplify their interface with ATE. Such a design allows external access to test activation pins and test points.

LRMs will be designed such that active component assemblies are not captive to their housings (i.e., with rivets or epoxy, by cable routing), thereby permitting their rapid disassembly/assembly.

Software Loading—Where applicable, LRMs should be designed to ease loading and downloading of software from the repair equipment. Surface data loaders should conform to ARINC Report 614, "Standard Firmware Loader for Avionics Shops."

Standard Bus Testing—At the spacecraft level, portable bus analyzers can be useful to support personnel for engineering analysis and maintenance functions. They can be used to verify the proper operation of the aircraft system buses and monitor message traffic.

Standard bus testing is also recommended for surface testing at the avionics module level. A high percentage of test coverage should be achieved. As a goal, bus testing should be able to isolate failures to the component level. The recommended commercial data bus is the IEEE Standard 1149.5 Test and Maintenance (TM) bus with boundary scan test.

3.4.6 Verification of Repair Action

Once the corrective action has been taken, there shall be a means of verifying the proper operation of the affected components. The spacecraft configuration database shall be updated to reflect maintenance actions and results.

3.4.6.1 On Spacecraft—The execution of a system-level functional test should provide a high degree of confidence that the affected LRM is serviceable.

3.4.6.2 In Surface Maintenance Centers—Verification of proper operation should be performed by executing the LRM's test procedure on ATE.

Section 4
COTS+ Architecture

4.1 COTS Components and Technologies

4.1.1 Space Candidate COTS+

This section identifies the domain of nondevelopmental and commercial components evaluated within this study. Representative types of COTS technologies, components, and systems are described to illustrate the advantages of using COTS and nondevelopmental items (NDIs).

Architectural and functional features of several Honeywell commercial and military avionic NDI subsystems considered to be candidates for space applications are presented herein. Although military avionic subsystems do not fit the strict definition of COTS, they are included to provide a more comprehensive assessment of the variances and complexities associated with the integration of COTS and COTS-like components in space applications. Therefore, the term *Space Candidate COTS+* will be used to describe both commercial and military candidate systems. This study will also include modified COTS components within the definition of Space Candidate COTS+.

Components and subsystems that represent expected technologies, characteristics, and integration complexities for a general COTS-in-space insertion were surveyed (see Table 4-1). Honeywell products were used because of the availability of data and the study team's familiarity with Honeywell product characteristics and descriptions. However, study results and conclusions are deemed applicable to all COTS and COTS-like subsystems. The incorporation of any or all non-Honeywell COTS and/or NDI components will be governed by requirements and restrictions similar or equivalent to those generated within this study. Further studies are recommended to evaluate the validity of the results herein for COTS+ products in general.

Data and analysis is provided in greater detail for four technologies selected for study emphasis. The four subsystems represent various technologies, configurations, components, and/or concepts that can be evaluated for space applications. Of the four subsystems, two are commercial airplane subsystems and two are military products. One military product is derived from commercial technology. The four technologies and subsystems and the reasons for their selection are as follows:

- Flat Panel Display Subsystem—The Boeing 777 airplane's active-matrix flat-panel display subsystem is used for analysis. The system is a commercial off-the-shelf product being designed and integrated by Honeywell for Boeing 777 aircraft cockpits. Flat panels represent components or subsystems involving new technology, man-machine interfaces (MMI), and unique safety-in-space requirements.

- Integrated Modular Avionics (IMA)—The Boeing 777 airplane's Airplane Information Management System (AIMS) is used to exemplify integrating modular avionics (MA), MA interfaces, and MA cabinets. AIMS is also a commercial off-the-shelf product. The AIMS is composed of dual integrated processing and I/O hardware cabinets that provide flight management, display interfaces, onboard maintenance, integrated condition monitoring, communication management, data conversion gateways, and engine data interfaces.

Table 4-1. Space Candidate COTS+

Related Honeywell COTS+ Products and Technologies
• Inertial navigation system with embedded GPS
• Six-sensor dual-fault-tolerant inertial navigation system
• Fiber-optic gyros
• Digital map
• Central maintenance system concept
• SAFEbus™
• Optical disk storage system
• Inertial reference system
• Production line automated diagnostics doncept
• Flight control maintenance diagnostic system
• Flat-panel display subsystems
• Smart sensors and actuators
• Pressure devices (air data)
• Inertial measurement unit
• Airplaine Information Management System
• Integrated INS/GPS
• Collision avoidance systems

The AIMS incorporates two state-of-the-art aircraft-unique fault-tolerant networks: the SAFEbus™ backplane bus and the ARINC 629 intercluster bus. It also incorporates ARINC 429 and optical FDDI networks as well as the Honeywell central maintenance concept listed in Table 4-1.

- Optical Disk Storage System—This high-density digital memory unit represents a fully militarized nondevelopmental item. This product was designed specifically to survive rugged military environments. Because it did not evolve from the modification or hardening of a commercial off-the-shelf design, it provides an example of changes necessary to modify or upgrade military equipment to higher space qualification levels. Application of optical disk technology within this report is useful to examine requirements and methodologies necessary to track and transition ongoing technical developments and improvements for space applications.

  Optical disk hardware exemplifies the complexities associated with using or qualifying for use in space devices that physically move and/or rotate and exhibit mechanical operations sensitive to vibration, acceleration, and shock environments. It also provides further evaluation of laser technology in space.

- Integrated INS/GPS Subsystem—This militarized nondevelopmental item was developed by integrating two separate subsystems (Honeywell INS and Texas Instrument GPS) to form one product.

As shown in Table 4-2, these four subsystems exemplify COTS components of different avionic type, characteristics, and technologies. Detailed descriptions of the four subsystems and the several Space Candidate COTS+ products, systems, and technologies listed in Table 4-1 are provided in Appendix A.

4.1.1.1 Flat-Panel Displays—Liquid crystal displays (LCDs) are now being designed for aircraft cockpits. The LCD display medium has significant advantages over cathode ray tubes (CRTs), and the liquid crystal technology has matured rapidly over recent years so that it can be committed to production programs. The advantages of LCDs over CRTs are:

- Less space required,
- Significantly lower weight,
- Less power consumption,
- Increased reliability,
- Increased readability in direct sunlight.

Table 4-2. COTS+ Technologies, Interfaces, and Systems

Technology	Distinguishing Characteristics
Flat-panel display	MMI and safety
AIMS	Electrical
Optical disk	Mechanically moving
INS/GPS	Militarized NDI

Liquid crystal displays provide a good example of how our space program may immediately benefit from using COTS hardware in space. If space avionic requirements and architecture can accommodate LCDs in their present form or accept slightly modified commercial systems, the insertion time to incorporate flat-panel technology in space should be considerably shortened. It is further desired that the requisition and logistical management of COTS LCD systems would not adversely affect the insertion process by requiring additional time-consuming procedures and requirements.

If, in addition to requirements and architectural changes, modifications to the commercial designs are required, a benefit is derived when required modifications are unconditionally incorporated within the commercial design. Thus, if commercial products were modified to incorporate required space application modifications with little or no extra cost, the two products are obviously identical. In this case, the modified product reverts to a COTS classification since it comes off the commercial line. Developing technologies such as the flat-panel subsystem are good candidates for such a scenario.

Immediate applications in the orbiter, transfer vehicle, and excursion vehicle cockpits can be found for the multifunction control display units (MCDU), the electronic instrument displays (EID), and electronic library system displays (ELS) for avionic and the flight/navigation management systems. The flat-panel technology provides a display unit (CDU) with eight colors, high-contrast, crisp definition, and excellent off-axis viewability for multifunction control display units and dlectronic instrument displays. The electronic library system displays currently use half-page, high contrast, monochrome technology to maximize resolution for reading fine detail.

Active-Matrix Flat-Panel Displays—Active-matrix liquid crystal displays (AMLCDs) are now being designed by Honeywell for aircraft cockpits. This new display medium has significant advantages over CRTs. The LCD technology has matured rapidly over the past 5 years so that AMLCDs can be committed to production programs. Honeywell believes AMLCDs will be the preferred choice for cockpit displays in the 1990s. Three cockpit display

applications are in development: primary flight instruments (EFIS/EICAS), small instruments/control panels (TCAS VSI/MCDU), and electronic library displays (ELS).

The major advantages of AMLCD technology are summarized below.

Volume and Weight—An important advantage of AMLCDs over current CRT displays is the reduction in both volume and weight of the display unit. A CRT contains many items that are not needed in an AMLCD-based display. The high-voltage power supply, cathode drive, and electron beam deflection amplifiers are no longer required for AMLCDs. The heavy CRT shielding and mounting materials are also eliminated. The fluorescent lamps and the light box required of the AMLCDs have low weight and volume. The minimum depth display will have the associated computational electronics placed in a host computer, and the remaining drive electronic in the unit will be reduced in size through VLSI techniques. Therefore the volume and the weight of an AMLCD is less than 50% of the same size CRT display.

Power—The significant portion of the power required in the AMLCD unit is consumed in the fluorescent lamps and lamp drivers and is a function of the brightness set for the display. The remaining power is used in the LCD row and column drivers and in the I/O and signal processing. Analysis of a D-size display unit shows that the lamp assembly consumes 20 to 25 W at a nominal brightness setting. The LCD drive requires 12 to 15 W, the I/O and signal processing use only 10 W, and the internal power supply dissipates approximately 18 W. Total power is estimated to be 60 to 68 W. This compares with 150 W (typical) for a D-size CRT display unit.

Passive Cooling—Because of the reduction in power realized with an AMLCD-based unit, forced air cooling of the unit is not necessary. By providing effective thermal heat paths and adequate surface area for convection, an AMLCD-based unit can be effectively cooled through natural convection. Direct thermal paths are provided between the cases of high-power electrical components and the external heat sink. This heat sink eliminates internal heat generated and provides structural support for the unit. Fins integral to the heat sink are optimized in terms of size and spacing. Even with this slight weight increase caused by the additional heat sinking needed for passive cooling, the AMLCD weighs much less than a CRT with the same size screen. In addition, if passively cooled flat-panel displays are adopted for all cockpit displays, the forced air cooling to the cockpit can be eliminated, further reducing the overall weight of the vehicle and the cost of the cooling system.

Reliability—Reliability of AMLCD will be twice that for CRT displays, which means an MTBF of 18,000 hours or greater. The LCD panel is very reliable, and the fluorescent lamps are designed for long life. System partitioning leaves very few electronic parts in the display unit, and the parts that remain will be mostly very large scale integrated circuits (VLSIC). Improved self-test and some redundancy will assure high availability of the equipment.

Improved Safety—AMLCDs eliminate some of the safety hazards associated with CRTs. Because they do not contain a vacuum, there is no danger of implosion; therefore, AMLCDs do not require a bonded implosion panel or tension band. AMLCDs do not require high voltage to operate, so arcing (especially at high altitude) is not a safety issue. Likewise, AMLCDs do not represent an implosion or shock hazard for repair personnel. X-ray emissions, which are generated in a CRT, are completely eliminated with AMLCDs.

Environmentally Rugged—Unlike CRT displays, AMLCDs are not affected by the earth's magnetic field or other magnetic fields produced on the flight deck. Therefore, AMLCDs will not have convergence problems from external magnetic fields and will not require the special shields used with CRTs. AMLCDs also have inherent immunity to the harsh environment that exists on the vehicle flight deck. This immunity is a direct result of the solid-state nature of the LCD panel and the ease of packaging it in a solid position because of the flat profile of the LCD panel face versus the curved profile of a CRT. Because the LCD panel is ruggedized and can be mounted flush in the chassis, the AMLCD becomes immune to any alignment problems caused by vibration. The fluorescent lamps are also mounted solidly and have no alignment requirements.

AMLCDs do not have any deflection circuits, convergence yokes, or a high-voltage generator, and the video signals are all at logic level, thus making the circuit designs for the display unit more immune to any magnetic or electromagnetic interference. The passively cooled packaging, which effectively seals the whole assembly also blocks EMI and electromagnetic emissions.

HERF and Lightning Protection—The digital nature of the AMLCD module makes it an attractive candidate for using a fiber-optic data interface to the remote drive electronics. With fiber-optic cable, light is transmitted through the glass medium rather than electricity through a metallic wire medium. The transmitted light signals are not distorted by any outside electronic, magnetic, or radio frequency interference. Optical fiber systems are intrinsically immune to lightning strikes and High-Energy

Radio Frequencies (HERF). The fiber-optic cable is also a nonconductive material; hence, it will not generate any cross-talk between adjacent transmission lines, and signals on the cable will not be a source of EMI.

Enhanced Maintenance—Once installed, AMLCD units are easier to maintain than CRT displays. AMLCDs are designed to make replacement of the backlight assembly simple. The lack of adjustments for purity, convergence, focus, and deflection mean that there are no sensitive adjustments or calibrations that must be done in the field.

The in-line assembly construction makes disassembly and repair times shorter and allows for easier troubleshooting. No special handling or tools are required. Because of the limited electronics in the display unit and the solid-state digital design, the BITE and monitoring can provide essentially 100% coverage for detection of failures.

Manufacturability—AMLCD units are simpler and easier to manufacture than CRT displays for several reasons. An LCD panel is flat and can be readily mounted into a display chassis. A CRT is large, bulky, and difficult to mount. A CRT must be mounted with a resilient material to prevent implosion of the CRT during shock and vibration. An AMLCD does not require high voltage; hence, potting tools and processes required to pot anode leads, CRT base leads, and high-voltage power supplies are not required. Bonding cover glasses and filters are simpler for LCD panels because they present a flat surface for the bonding material. This means that the bonding material can be thinner than that for a CRT. Furthermore, since the bonding material will be of uniform thickness, mismatches of thermal expansion coefficients between the AMLCD and the bonding material are less of a problem (i.e., the bonding material will not pull away from the cover glass).

Because AMLCDs are not susceptible to the effects of the earth's magnetic field and other magnetic fields generated on the flight deck, they do not require a magnetic shield in the display unit. Magnetic shields for CRTs must be handled carefully during production or their magnetic shielding properties will be compromised. Since AMLCDs do not require adjustments for purity and convergence, AMLCDs are also easier to test and calibrate in production.

Larger Display Surface—The desire for larger displays in all glass cockpits has been frustrated to an extent by limits in CRT technology. Larger CRT displays typically translate to deeper display units with more display surface curvature and a disproportionate increase in power per unit display area. With the exception of increased computational power and display memory size, which are both accommodated by recent advances in semiconductor technology, larger AMLCDs do not pose any limitations in terms of physical display size or power.

In addition, CRTs are notoriously inefficient in extending the active display surface to the boundaries of the bezel for two primary reasons. First, the CRT bottle and the mounting of the shadow mask preclude the active area from extending out to the edge of the bezel. Second, because the CRT display surface is recessed below the bezel surface to accommodate the contrast enhancement filter and the display surface curvature, the active area must be designed smaller to prevent the bezel from occluding the view. AMLCDs are flat regardless of their size so that the display surface can be placed just behind the bezel surface, and AMLCDs can be designed with active areas out to within 2 mm of the display bezel.

Better Display Viewability in Bright Sunshine—Even with contrast filter enhancement, a CRT display's contrast ratio can fall to just 3:1 in bright sunshine. AMLCDs, which intrinsically absorb rather than reflect incident light, improve this contrast ratio by a factor of 3:4 without resorting to any special configurations. In addition to contrast ratio in a color display, color discrimination is a very important index of display readability. AMLCDs outperform CRTs in this regard as well. Because an AMLCD is less reflective, the colors are not as de-saturated by bright sunshine, making color differentiation much better.

Enhanced Display Formats—The AMLCD may be considered a full raster type display as opposed to hybrid stroke/raster displays that are currently being used. The essential distinction is that there is no fundamental limit to how much can be drawn on the display. CRT systems can display only a small amount of symbology measured in inches per second. In a stroke system, each vector or line must be drawn individually at a speed limited by deflection power and bandwidth. Because the brightness decreases with writing speed, the CRT display will become insufficiently bright if too much symbology is drawn.

The AMLCD allows the quantity and variety of graphics effects to be much richer using the AMLCD panel because each pixel can be controlled. Only a limited amount of raster symbology is feasible with the CRT hybrid/stroke raster systems. The all-raster capabilities of the LCD provide opportunities to enhance the display symbology.

One such enhancement is the use of a raster to draw thermometer-type scales. This type of scale typically is used for engine parameter tapes. CRT systems have implemented this type of display by drawing several stroke lines closely spaced. This implementation creates a narrow and

bright stripe for the tape. The desired tape is wider and dimmer. The AMLCD raster can easily create wide tapes of any desired brightness or contrast because of the variable brightness control of every pixel. The rastered thermometer-type display may also be used to draw effective airspeed limits.

The AMLCD also allows background raster areas. This background rastering is used to a limited extent with CRT displays to enhance readability of scales, but CRT systems allow only a few areas to be rastered on each display. The LCD suffers from no such limitation. The entire background area may be rastered (use of a background that is not black may reduce eye fatigue) or many separate areas may be rastered. Background rastering also allows the use of pop-up windows, where the window is separated from the main display by a different color background. These pop-up windows may be used for several different types of functions, including alerts, alternate windows (FMS performance data on a navigation display), or ACARS messages.

AMLCD raster displays can also display inverse video in which the background is bright and the symbology or text is black. This type of inverse video display is impractical with stroke displays. Inverse video is very effective for emphasis (alerts, required pilot actions, etc.) or highlighting pilot selections.

AMLCD raster displays also allow haloing of characters. Haloing creates a very narrow, dark boundary around each character. This dark boundary is very effective in reducing clutter and improving readability of the symbology. This haloing technique is especially effective in decluttering map displays where text or symbology from adjacent map features often overwrite each other or overwrite background raster field data such as weather radar.

AMLCD raster displays inherently allow the use of bit-mapped graphic characters. Bit-mapped graphics describe each character as a collection of small elements. Bit-mapped graphics allow for filling characters (filling characters with a stroke system requires many overlapping strokes and much writing time). Additionally, many commercial graphics applications use bit-mapped graphics; consequently, system development effort is reduced and performance improved by the availability of commercially developed graphics chips and software.

The AMLCD raster display is inherently compatible with other raster displays. This compatibility allows for video overlays of television or FLIR data. Additionally, it is possible to display graphics data, such as weather maps or navigation charts, that may be uplinked or prestored in an onboard electronic library system.

Installation Flexibility—The AMLCD offers great installation flexibility. The shallow depth and passively cooled construction of the display unit allows it to be easily installed in a variety of vehicles. The AMLCD may be considered as two modules: the actual display module itself, which is very thin, and the drive electronics. The display module outline is constrained by the desired display area, while the drive electronics may be packaged in whatever outline is required to fit in the vehicle.

The AMLCD's relative immunity to environmental factors also eases installation. The AMLCD is immune to the magnetic and electronic effects of adjacent electrical/electronic devices which have proven troublesome in the installation of CRTs. The low power dissipation of the AMLCD allows for passive cooling, and thus no plumbing such as cooling air hoses is needed. In summary, installation of the AMLCD is considerably simplified.

High Connectivity—Switching of display information to several different display units can be accomplished easily if the data on the interface is digital and a simple protocol is used. AMLCDs, which are inherently digital, are able to achieve high connectivity and still have a simple low-power, low-weight display unit. The basic approach to the interface definition is to design a minimum-complexity display unit and to transmit a TV-like signal using a standard bus protocol over a fiber-optic bus with a bandwidth above 100 MHz.

The principal advantage of this high-connectivity approach is greater flexibility in the flight deck configuration. One display management computer (DMC) is capable of driving multiple displays of varying types via a standard bus interface. High interconnectivity also improves the display system availability since it provides more options for reconfiguration.

4.1.1.2 Integrated Modular Avionics—This paragraph specifies an important part of the COTS+ space avionic architecture—a commercial integrated modular avionic concept that represents a significant part of COTS+ hardware, software, and networks. The IMA concept described herein is eventually networked together with LRUs in a bottom-up insertion of commercial architecture and used as an architectural point of departure for this study.

To the greatest extent, two sources of commercial aircraft modular architectural requirements are used herein to define space integrated modular avionic requirements. ARINC IMA guidelines and Boeing 777 architectures are used to establish our spacecraft point-of-departure requirements, since these commercial architectural requirements provide the means whereby commercial subsystems may be incorporated in space systems.

This study will use the Boeing 777 airplane's AIMS design as the primary reference for integrated modular avionics definition. The AIMS design is more representative of certifiable, production-ready IMA architecture than are the ARINC guidelines. The ARINC guidelines referenced in this study are preliminary and subject to changes, recommendations, and inputs derived from applications such as AIMS.

AIMS—The AIMS is a representative implementation of an integrated module cluster for space-vehicle avionic architectures. AIMS integrates the following functions in two cabinets:

- Electronic flight instument system/engine indication and crew alerting system (EFIS/EICAS) display generators;
- Flight management;
- Onboard maintenance (including airplane condition monitoring function (ACMF) per ARINC 624);
- Communication management;
- Data conversion gateways.

AIMS was selected for assessment within this study because it provides the space vehicle with a ready-made fault-tolerant avionic subsystem. The AIMS operating system and hardware provides total function separation and isolation under a combination of partition errors. It prevents application software from controlling shared resources to the exclusion of other application software (time partitioning), prevents application software from contaminating memory areas of other application or operating system software (space partitioning), and prevents failure of a hardware element unique to an application from affecting another application.

The AIMS provides maximum use of sharable resources and common designs, efficient implementation of multiple criticalities, computational integrity, and reduced life cycle costs through step improvements in maintenance diagnostics, removal rate (no fault found), dispatch reliability, and product reliability. Within two cabinets, AIMS provides partitioning between critical (10^{-9} unreliability), essential, and nonessential functions.

ARINC IMA—Guidelines/requirements from Project Paper 651 are used to fill in requirement detail. In the event of conflict between requirements ARINC and AIMS, either the ARINC requirements will be specified in lieu of the AIMS, because the AIMS design is presently proprietary, or an assessment will be made by study authors to select the requirement best fitting the definition from the MPRAS study or recent U.S. Government-sponsored avionic studies such from General Dynamics, Martin Marietta, and Lockheed Sanders.

Module Clusters—The COTS+ architecture provides for IMA cabinets networked to other IMA cabinets and LRUs. These cabinets (described in Subsection 4.3) represent the standard module enclosures necessary to implement RDIs and module clusters. The cabinets provide mechanical and electrical interfaces for standard modules and/or custom modules in module clusters.

The following paragraphs describe and specify standard module functions and components that are a part of the cabinets. IMA electronic modules, network/bus interfaces, software, and cabinet description/requirements are included herein.

Core Processor Module—Many of the detailed requirements for the processor module depend on IMA architecture and will not be common for all architectures. For example, a multitasking processor module will require more stringent requirements than a distributed processing module, especially in areas such as processing performance and robust partitioning. The cabinet designer/integrator is responsible for ensuring that a particular processor module design addresses the appropriate criteria for the specific IMA architecture being considered. The detailed characteristics of the processor module are (TBD) defined in ARINC Characteristic 7xx.

The processor module contains the computational capability for the functional applications installed in a particular cabinet. Identical processor modules with only one part number can be used in all cabinets, or more than one processor module implementation may be developed. It is desired that the most capable processor modules be developed and implemented for IMA cabinets. This will ensure that the processor module will have the greatest potential application and a large growth capability. All processor module types will be capable of operating in any cabinet. The specification of the processor module and all its interfaces will ensure electrical and protocol compatibility with respect to the cabinet backplane.

The processor module employs a method of fault tolerance that is transparent to the application software for faults in shared resources. Each application manages the fault tolerance details in its application-specific or private resources. As a minimum, the core module failure response is fail-passive.

The processor module will be programmed in Ada as a common high-order language. Refer to Subsection 4.4, Software Design, for software design considerations.

Processor—The processor module provides the maximum processing performance available from the latest generation of high-throughput microprocessors. Arithmetic

accelerators such as coprocessors, floating-point units, and cache memories are used where appropriate to enhance performance and reliability and reduce cost. Cabinet growth and flexibility in an IMA environment is very dependent on processor module performance. The efficiency of the architecture improves as levels of integration increase.

Where floating-point operations are supported in the processor module, they conform to a standard format. Because of its widespread acceptance in the integration of floating-point units on contemporary microprocessors, ANSI/IEEE STD 754 is the preferred floating-point format.

I/O for the processor module will be implemented in a protected manner in support of robust partitioning.

Robust Partitioning—The processor module includes mechanisms that enforce separation and provide a robust logical boundary between the partitions resident in the cabinet. This protection ensures that no one partition can adversely affect another. The entire architecture shall be carefully designed to extend this protection throughout the cabinet, including the I/O areas. The applications will not be capable of compromising these protection mechanisms.

Memory management hardware is included in the processor module to provide separation and protection for I/O resources and each application's memory space. The memory management hardware is often integrated into the processor module's microprocessor. Control tables used by the memory management hardware are fixed in memory according to the analyses and decisions made during the design process, and are implemented in nonvolatile reprogrammable memory. The ability to modify these tables is interlocked and safeguarded so that unintentional alternation is not possible by the executive or operational software. This requirement assures a high degree of integrity to the design.

A programmable, time-interval interrupt generator gives the processor module the capability to partition and protect applications in the time domain.

Memory—The processor module contains enough nonvolatile memory to store all of the application programs, typical amounts of data that would be assigned to any cabinet, and enough scratch pad random access memory (RAM) to handle any combination of assigned functions. A smaller amount of nonvolatile memory available for use by the cabinet maintenance function to implement error logs and fault histories. The processor module design includes provisions for accommodating unique applications that use very large data stores.

Like processor performance, the processor module's memory capacity directly affects the IMA cabinet's flexibility to incorporate future growth. The processor module design maintains a large reserve growth margin in the memory area.

Software Reprogrammability—All aspects of the core software that need to be altered to add or upgrade functions are to be reprogrammable in-circuit through onboard software loading. The application software load will occur via the backplane interface and only be enabled after the proper safeguards and interlocks have been verified. The following software is to be reloadable:

- Programs in nonvolatile memory,
- Data in nonvolatile memory,
- Memory management tables,
- Backplane bus tables,
- Any other control data tables that allocate processor time or other core resources.

Interface Specification—Core modules shall meet the applicable specifications for the following standard interfaces:

- Interface to the global bus,
- Interface to the backplane buses,
- Interface between the executive and the functional software modules,
- Hardware and software interfaces to support the cabinet maintenance function (BITE),
- Interface to the onboard cabinet data loader.

Backplane Data Bus Interface—The backplane data bus interface shall support all modes of the operation. Both control of and the interface to the backplane data bus are accomplished in a fault-tolerant manner so that failure of the interface or control circuitry causes no loss of that bus. The design of this interface minimizes an application's involvement in monitoring and redundancy management as much as possible. The backplane bus interface provides fault detection, isolation, and reconfiguration for failures of the backplane bus itself, making bus faults transparent to the application software. The design of the interface supports applications and databases with all levels of criticality.

Power Supply Modules—The detailed characteristics of the standard power supply module will be defined in ARINC Characteristic 7xx. This subsection describes the architectural requirements of this module.

Each power supply module has two power input line pairs. The pair uses standard aircraft input power, voltage level, and tolerance (power standard) as defined in the ARINC characteristic.

Each power supply module has separate output power line pairs for each cabinet LRM. Each pair has independent overcurrent protection so that an overload (including a short circuit fault) on the power line to one user module does not degrade the power to any other user module. The power supply module is capable of reporting the status of any overloaded output.

The cabinet designer/integrator is responsible for ensuring that the number of redundant power sources available to each user module is appropriate to the integrity requirements of the system(s) dependent on that module. The installer is responsible for ensuring that the independence of the power sources to the power supply modules in a cabinet is appropriate to the integrity requirements of the systems dependent on those modules.

The power supply modules will have some form of heat sink or heat exchanger to operate in the cabinet. Since the heat rejection requirement of any power supply is largely dependent on the power level it supplies, and since the loads are normally shared, it has been suggested that pairs of power supply modules be mounted so as to share heat exchangers. Heat exchangers should be designed to handle worst-case power load resulting from one power supply failure in the cabinet.

Standard I/O Module—The COTS+ IMA approach infers a number of standard I/O modules. This includes all of the I/O types for which there is a general need throughout an vehicle. This may include or refer to a specification for a standard sensor or other vehicle standard interface specifications. This section describes the desired capability of I/O LRMs.

Standard I/O LRMs shall be developed to interface with the vehicle. Each LRM may provide interfaces to a single type of signal or to some optimum mix of signals with some software programmable/reconfigurable selection of signal interfaces. These should be designed to support the most critical functions. A single failure within the LRM should not result in the loss of more than one of the I/O channels. The outputs should be fail-passive in nature.

It is the aim of IMA architecture to minimize the number of specific I/O types. However, this may not be practical and cost-effective for the foreseeable future. It is, therefore, proposed that at least the following three types of standard I/O LRMs be defined for interfacing the IMA cabinet with other vehicle systems:

- ARINC 629 I/O
- Serial and analog discrete I/O
- Bus bridge and gateway

Several types of standard I/O functions are provided within these three standard I/O modules.

ARINC 629 Interface—The ARINC 659 interface module interfaces multiple ARINC 629 data buses to the ARINC 659 backplane bus and include a bus bridge function.

Serial and Analog Discrete Interface—This module has the ability to interface with a combination of low-speed serial, analog, and discrete I/O channels of the vehicle. The number of I/O channels (serial, analog, or discrete) is standardized for each type of I/O. The LRM will have programmable features to define characteristics of input or output signals at each of the I/O pins under software control. The following generic types of I/Os are supported by this LRM:

- Analog Input Interface—This module is capable of interfacing with vehicle standard AC and DC signals. The LRM will perform necessary signal processing of the inputs and provide the digitized outputs to the core processor.

- Analog Output Interface—This module will be capable of performing the functions of a programmable arbitrary waveform generator and provides standardized output signals.

- Discrete Input/Output Interface—This module will be capable of being interfaced with commonly used vehicle discrete inputs and will provide similar discrete outputs for interfacing the IMA cabinet with other vehicle subsystems. Specific characteristics of each I/O signal will be downloadable via the backplane bus from the core processor module.

- ARINC 429 Interface—The ARINC 429 interface will be capable of either accepting or transmitting data at a selectable rate of ARINC 429. This interface could be a subset of programmable analog or discrete I/Os.

Bus Bridge and Gateway Modules—Bus bridges and gateway functions shall be implemented as standard I/O modules.

Special I/O Module—Where special signal types or interface requirements cannot be met with a standard I/O LRM, it will be necessary to design a special I/O LRM. It shall contain only circuitry that is necessary to meet those requirements. The rest of the task should be performed by an accompanying software application in the core processor. In all cases, these LRMs shall meet the same backplane bus interface characteristics as a standard I/O LRM.

4.1.1.3 Optical Disk Subsystem—A Honeywell optical disk module is included as an example for using COTS+ mass memory storage products in space. Optical disk mass memory storage provides an advanced form of data storage exhibiting a relatively high degree of ruggedness. It would replace the magnetic tape subsystem now used for mass memory technology for space.

During its years in the commercial marketplace, the magneto-optic (MO) rewriteable media used in tactical data cartridges (TDCs) has demonstrated a high level of reliable performance providing essentially infinite (greater than 1 million) write-erase cycles. The media substrate is a tempered glass that provides full performance operation in military aircraft vibration, acceleration, and temperature environments.

Glass also has excellent flatness and optical properties, and it protects the recording layer from hydroscopic moisture intrusion. Because the recording layer is fully encapsulated, the archival life of stored information has been demonstrated to be greater than 10 years. The full functionality of glass-substrate-based media has been demonstrated in thousands of flight hours in production aircraft.

Further details on the characteristics of the optical disk subsystem, its performance, and its advantages compared with other technologies are presented in Appendix A.

Mass Memory Storage Module—The mass memory storage module provides a fault-tolerant mass storage capability necessary for permanent storage of application programs and databases. Application software is to be loaded from the memory's application module into processing modules when needed. The memory unit is also used as a storage device for navigation databases (maps, star catalogs, etc.) and an electronic library to support specific applications such as the onboard maintenance system, charts for navigation and communications, and in-flight training aids.

Application Function—The known advantages of using a mass storage module for permanent application storage are flexibility in reconfiguration and high reliability. The application software can be stored permanently in a mass storage module and downloaded to the processing module when needed. This data exchange shall be controlled by the processing module.

Separating the permanently stored applications in a high-density mass memory storage unit and the processing module provides more flexibility during failure recovery because there is no fixed relation in location between the applications and the processing mode. Alternate concepts using smaller mass memory modules located within user processor cabinets or requiring that the core module processor contain sufficient unpopulated growth capability to allow adding large database memories to the module as needed are deemed less flexible and cost-ineffective.

Database Function—The database information necessary to support specific applications can be loaded from or saved in the mass storage module when needed. This data exchange will be controlled by the processing module using the data.

Memory—The memory of the mass storage module consists of a large, high-density, environmentally hard, nonvolatile memory. The nonvolatile memory provides permanent data storage for applications and/or databases. Each application or database is loadable without removal of the modules.

The nonvolatile memory provides buffer memory to support:

- The interface between the mass storage module and processing module volatile memory.
- Storage of status information dedicated to the application being executed by the processing module to create a smooth reconfiguration transition after failures.

Mass Storage Controller—A mass storage controller residing within the mass storage module controls information flow, failure detection, failure isolation, and reconfiguration strategy inside the mass storage module.

A part of the mass storage controller provides partitioning between the applications, databases, and partitions thereof to allow applications or databases of different criticality levels in the same mass storage module.

The partitioning function is a hardware function driven by the software part of the mass storage controller.

Fault Tolerance—The level and type of fault tolerance depends on the criticality level of the applications or databases and the maintenance considerations. The fault tolerance could be achieved by multipath possibilities initiated by the mass storage controller or a processing module.

Application or Database Loading—All applications or databases are loadable through onboard software loading. The loading process of the applications or databases will be initiated by a processing module via network interfaces, and the final location of the applications or databases inside the mass storage module will be organized by the mass storage controller.

4.1.1.4 Integrated INS/GPS—The integrated INS/GPS assessed within this study uses recently developed militarized NDI technology. Assessment of an integrated INS/GPS within the COTS+ study architecture provides an evaluation of an LRU that provides distinct advantages to the space vehicle:

- The military-grade INS/GPS uses electronics that come off a production line that produces both military and commercial components. This study will determine if the cost savings realized for military applications are more or less applicable for space applications.
- Accurate pseudo-range and range rate data are not available from a stand-alone GPS receiver because of selective availability (SA). SA is the intentional degradation of satellite-transmitted measurement data. The National Security Agency (NSA) or the Department of Defense (DoD) control its implementation and activation. At this time, the degradation causes approximately 100-m accuracy errors. NSA-authorized receivers have a precise positioning system–security module (PPS–SM) that removes the SA errors, yielding accurate GPS navigation. However, the NSA does not allow a stand-alone authorized GPS receiver to transmit accurate pseudo-range and range rate data on a data bus external to its own chassis. To take full advantage of GPS measurement data, the Honeywell H764-C3 INS/GPS has embedded the receiver. NSA does allow internal transmission of receiver measurement data.

The INS/GPS can be used as a point of departure navigation subsystem from which other navigation subsystems using emerging/developing technologies can be evaluated for COTS+-in-space applications. The advantages of fiber-optic gyro (FOG) and miniature GPS receiver (MGR) subsystems in space have been cited, and products incorporating their technologies in integrated or separate designs are being developed. These products, including the Honeywell ARINC 743 GPS/GLONASS sensor unit being developed in cooperation with the Soviet Union, would be likely candidates for near-term COTS+ insertion. Expedient future modification of the INS/GPS definition to include any or all of these technologies is possible.

4.2 Supporting Commercial Technologies

4.2.1 Introduction

The COTS+ in space architecture is based on the application of established commercial technologies that, together with Integrated Modular Avionics (IMA) (ARINC 651), can be applied to form a complete system. This subsection describes previous mentioned and several other elements that are fundamental to the COTS+ concept; more detail is provided for technologies used in the COTS+ strawman architecture. The technologies described in this subsection are:

- ARINC 653: Application Software Interface;
- ARINC 659: Backplane Data Bus—SAFEbus™;
- ARINC 653: Application Software Interface;
- ARINC 652: Software Management;
- ARINC 650: Packaging Concepts;
- ARINC 638: OSI Upper Layers;
- ARINC 637: Internetworking;
- ARINC 636: Onboard Local Area Network;
- ARINC 629: Data Bus;
- ARINC 624: Onboard Maintenance System;
- Project Paper 167: Certification and Configuration Control;
- ARINC 613: Ada;
- ARINC 610: Flight Simulator Avionics;
- ARINC 609: Electric Power;
- ARINC 429: Data Bus;
- Related Documents:
  - EUROCAE ED-14x,
  - EUROCAE ED-12x,
  - RTCA DO-160x,
  - RTCA DO-178x,
  - RTCA DO-205.

4.2.2 Data Buses

Commercial aircraft data bus standards have evolved somewhat independent of the DoD aircraft standards, since the two types of aircraft have had vastly different requirements for interunit and intraunit communication. The development of commercial standards has been driven significantly by certification requirements.

The evolution began with the introduction of ARINC 429 and has resulted in the recent emergence of ARINC 629 and the Honeywell-defined SAFEbus™. At the time of this report, the Honeywell SAFEbus used in the Boeing 777 airplane's Aircraft Information Management System (AIMS) has become the leading candidate for adoption by the Data Bus Subcommittee.

4.2.2.1 ARINC 659: Backplane Data Bus—Intracabinet communication is performed using the ARINC 659 backplane data bus standard. ARINC 659 is a data bus designed for medium-level data throughput inside the avionics cabinet. The bus has specified maximum line length and impedance and a standardized bus driver/interface. All cabinet modules are expected to conform to the ARINC

659 interface standard. The details of the backplane data bus are documented in ARINC Specification 659, Backplane Data Bus.

Backplane Bus Characteristics—The ARINC 659 backplane bus is characterized by several parameters that ensure compatibility at the interface. The physical attributes of the bus include the number of wires associated with it together with its signal levels and timing requirements. The bus message structure attributes consist of address/label structure, word bit significance, string structure, error provisions and message acknowledgment capability.

Speed—The bus supports the bit rate estimated for an avionics cabinet plus a growth capability of 100%. The bus speed can be determined by I/O data traffic and intermodule communication in multiple-core cabinet configurations. Analysis shall consider encoding, addressing and error detection over and above the basic data bit rate. Speed shall be determined by a defined message structure, transmission frequency, error detection and correction capabilities.

Integrity/Availability—To support the integrity and availability needs, the bus provides error detection, parity and string checksums, CRCs, together with error correction, access violation, detection, impersonation detection, memory violation protection, data consistency checks and reconfiguration control.

Structure and Redundancy—As a minimum, dual independently operating buses are used. Each is independently monitored on the basis of self-test and status data received over the bus.

This structure allows flexibility in redundancy management in that the redundancy provision can be tailored to the specific application at hand. Bus provision is 100% by limiting the bus traffic under normal operation to 50% of installed capacity. Each bus is a single monitored bus with access protocol monitoring and bus coupling provisions directed toward preserving the function of the bus.

Features—The ARINC 659 backplane bus offers the benefits of flexibility, commonality and maturity. The requirements for the backplane are such that the ARINC 659 standard may be applied to offer flexibility in an economic way. The desired features include:

- High bus loading without clash,
- Guaranteed periodic access,
- Protection against impersonation,
- Message overrun protection,
- Predictable operation,
- Broadcast and directed data transfers.

4.2.2.2 SAFEbus™ Backplane Bus—Honeywell has designed SAFEbus, an innovative serial backplane bus to provide communications of all data between the modules in the Boeing 777 AIMS cabinet. SAFEbus supports multiprocessor architectures. SAFEbus is being developed because no existing protocol adequately meets all key requirements of a bus (i.e., time determinism, memory protection, high-performance, high efficiency, low pin count, and total fault containment). The standard also provides additional support for conducting debug, verification and certification operations.

The SAFEbus interface logic consists of a bus interface unit (BIU) ASIC, and EEPROM table memory, and intermodule memory and backplane transceivers. This logic is paired to provide full concurrent monitoring. All communications between application code in processing modules and other modules is via messages that are assigned to fixed buffers in the intermodule memories. The modules simply view the bus as a protected memory-mapped peripheral.

The SAFEbus protocol is driven by sequences of commands stored in EEPROM table memories. The BIUs in every module on the SAFEbus are synchronized to the same point in their respective tables, and mechanisms are provided to quickly regain synchronization if it is ever lost. Bus time is divided into a set of windows, each containing a single message from 32 to 8192 bits in length.

The windows are separated by a fixed gap time. The command in each BIU's table that corresponds to a window indicates whether the BIU should transmit, receive, or ignore (a skip command) the data during the time assigned to that window. The tables also contain the intermodule memory address of the data to be either transmitted or received. The commands are organized into cyclic loops (frames) of constant length set by the sum of the individual window lengths.

One of the unique benefits of the table-driven SAFEbus protocol is its extremely high level of efficiency. Because all of the fixed location and window assignment information is kept in tables, assignments do not need to be transmitted on the bus.

The lack of arbitration also reduces the nondata overhead. Except for the intermessage gap (two bit times per window) and the occasional synchronization messages, all remaining bits are data. Thus, for a continuous stream of 32 bit messages, SAFEbus is more than 94% efficient. Most existing serial protocols perform very poorly for such short messages, typically in the 10% to 30% efficiency range. Backplane messages of this length are quite typical in avionics applications (those generated by ARINC 429, for example). It is this high level of efficiency that enables SAFEbus to be implemented using a serial backplane.

The data on the SAFEbus is transferred at 30 Mbit/s (nominal) over dual self-checking buses (SCBs). Each of the SCBs is actually two serial buses, one driven from each of the duplicated BIUs in the transmitter module. The data on each bus in the pair is compared at the receiver. If a miscompare occurs, the data is discarded and not written into the intermodule memory. The transmitting module checks what it actually puts on the bus to detect errors. The dual nature of this comparison ensures that a babbling module cannot stay on the bus. The net result of the SCB approach is fault detection coverage that exceeds the coverage provided by CRC codes, without any throughput overhead.

The addition of the second SAFEbus SCB provides immediate error correction for transient errors on the backplane. It also enhances the cabinet availability since SAFEbus is fail-operational/fail-passive.

SAFEbus Determinism—All shared resources in the AIMS cabinet are rigidly partitioned to ensure that the various applications execute correctly under all possible operating conditions. Studies and work with the FAA have shown that strict deterministic control is the optimum way to meet the partitioning requirements for the backplane bus.

An additional advantage of partition/bus synchronization is the elimination of the need for most double buffering. It is possible to schedule the transmission of a data block only when it is known that the application software is not accessing or modifying it. This reduces intermodule memory requirements and makes speeds access to the intermodule memory.

Synchronization of the bus and software also benefits debugging and validation. First, the explicit time determinism of SAFEbus means that the system timing that a partition experiences is the same whether it is the only one in the chassis or whether it is running in a fully populated cabinet. Second, since processors are synchronized to the bus, they are implicitly synchronized to each other. Thus, any timing errors between partitions running in different cores will be exposed quickly, making it simpler to debug. In asynchronously scheduled multiprocessor systems, such timing problems appear as intermittents, which can be very costly to track and make it impossible to validate the system.

An additional benefit of the SAFEbus synchronism is that when the system is stopped or single-stepped, there is a simple relationship between the states of all of the partitions as defined by the SAFEbus table, making it easier to trace behavior. This degree of synchronization allows each BIU to maintain a 32-bit global timer that is used to time stamp intermodule memory buffers.

Summary of SAFEbus Attributes—SAFEbus uses table-driven protocol, which assigns time windows to each message, eliminates arbitration requirements, guarantees determinism and synchronization (to I/O and other processors), issues real-time interrupts, anticipates partition data requirements, eliminates address transmission requirements, thus increasing bus efficiency, and provides a structure for V&V and certification.

SAFEbus also features serial transmission with a minimum pin count, 30-MHz worst-case operation with 94% efficiency (anticipating 50-MHz, 2-bit-wide bus capability in the future).

SAFEbus relies on full concurrent monitoring through self-checking pairs. All transactions are performed by dual BIUs. This allows dual monitoring at multiple points and low-latency fault detection. There is total fault detection and containment of bus-related errors. Data is transmitted on two independent buses, and there is 100% correction for single-bit transmission errors with no error coding overhead. The redundancy of bus elements facilitates fault tolerance. The effects of a fault are contained by the self-checking pair mechanism in the BIUs and the cross connection of the transceiver enables, unless the fault is in the final stage of the transceiver. Any contained fault is easily isolated for maintenance purposes via the self checking pair trip indication.

4.2.2.3 ARINC 629: Data Bus—The ARINC 629 data bus is the preferred interface between commercial avionics cabinets and the sensors, displays, and actuators. The bus can be described as a serial bi-directional data bus system which is capable of transferring data at the rate of 2 Mbit/s. The bus is intended for use for functions having the highest criticality requirements as well as for nonessential functions. The detailed operation of the data bus is described in ARINC Specification 629, Multi-Transmitter Data Bus, Part 1, Technical Description.

The ARINC 629 Periodic-Aperiodic Multitransmitter Bus is a serial multiple-access data bus intended for use on commercial transport aircraft entering service in the 1990s. It is a masterless broadcast bus, like ARINC 429, operating on the carrier-sense, multiple-access, clash-avoidance protocol. It is the product of more than 30 person-years of research and development. Initially developed by the Boeing Commercial Airplane Company as Digital Autonomous Terminal Access Communication (DATAC) to be a potential successor to ARINC 429, the bus carries the designation ARINC 629: Periodic-Aperiodic Multi-transmitter Bus.

During its development, the trends in avionics architecture were investigated, and the requirements for a central data

communication system were established. In 1982, NASA Langley Research Center installed and flight tested DATAC hardware on the Boeing 737 Advanced Transport Operating System (ATOPS) airplane. This provided industry with an opportunity to gain flight experience with the data bus. In 1986, the Airlines Electronic Engineering Committee (AEEC) formed the Data Bus Subcommittee to develop the ARINC 629 data bus standard based on the Boeing DATAC design.

ARINC 629 is a high-integrity data communication system that uses a time division multiplexing protocol. The bus is intended to be applied to systems requiring a high degree of data integrity and moderate bandwidth. ARINC 629 employs a deterministic data transfer schedule mechanism to ensure unimpeded data communication for all systems under maximum bus load conditions. ARINC 629 conforms to Open Systems Interconnection (OSI) principles.

The ARINC 629 system can operate in broadcast mode and point-to-point mode at speeds up to 2 Mbit/s. At this rate, the theoretical data throughput is 100,000 data words per second. As applied to commercial avionics, ARINC 629 is capable of serving the following types of communications:

- Intersystem data communication where the data bus forms a data network and integrates participating systems by sharing memory resources.
- Intrasystem data communications for any system with a distributed architecture (sensors, controls, displays and actuators).
- Point-to-point data communications for sending data from a source to a single destination with positive message acknowledgment.
- Global bus performance, status reporting and system test capabilities to support future maintenance concepts.

The ARINC 629 protocol is implemented in a very large scale integrated circuit (VLSI) device. The output of the protocol chip is connected to the bus medium through a serial interface module (SIM). The data bus employs two different protocols for transmitting messages:

- Basic Protocol (BP)—essentially the DATAC protocol proposed by Boeing. It is capable of operating in two different modes: periodic mode and aperiodic mode. The periodic mode assures periodicity on the bus, and the order of transmission is dependent on bus initialization. The equal priority access rule is maintained even under overload conditions. If the bus is overloaded, the bus will automatically transition into the aperiodic mode of operation. The aperiodic bus assures order of transmission on the bus, however, update rates are determined by bus loading factors.
- Combined Mode Protocol (CP)—developed by the AEEC Data Bus Subcommittee to combine both periodic and aperiodic data transmissions on a single ARINC 629 bus. CP assures that the frequency of periodic transmission is maintained on the bus. It provides three levels of bus access priority that correspond to the priority level of the data transmitted on the bus:
  - Level 1—Normal periodic transmissions of constant-length messages. Transmission sequence on the bus is in ascending order of unique terminal gap (TG) allocation. TG is a unique timer assigned to each terminal on the bus. To avoid collisions on the bus, each terminal on the bus must have a unique TG.
  - Level 2—Infrequent, short aperiodic transmissions requiring access within one periodic transmission cycle. Only one level 2 transmission is permitted per transmit interval (TI). To ensure access in any TI for all terminals at level 2, CP buses are designed with sufficient available bus time, after the level 1 load is accounted for, to accommodate total bus occupancy. TI is a system-wide timing parameter that is set to the same value in all terminals. It is started in a given terminal at the moment the terminal starts transmitting. Once a terminal has transmitted, it waits the length of time specified by the TI before it can transmit again. This timer's value typically ranges from 0.5 to 64 ms.
  - Level 3—Low-priority aperiodic messages with a maximum length of 257 words. More than one level 3 transmission per minor frame is possible if spare bus time is available. Since available bus time may be insufficient for all terminals to transmit during the same minor frame, the bus protocol ensures that deferred terminals are given access in the following frame(s).

Both BP and CP are capable of transmitting broadcast messages and directed messages and have the capability to transmit bulk data such as navigation databases. For a bus using BP, bulk transfer is performed by having the terminal assume an alternate transmit schedule. The transmit terminal resumes its primary transmit schedule when the bulk data transfer is complete. Depending on the amount of file data to be transmitted, a periodic bus may transition to the aperiodic mode. For a bus using CP, file transfer can be handled by structuring the data in a series of single block aperiodic messages.

There are several similarities between 629 and MIL-STD-1553. Each word is 20 bit times long with 16 bits of data and a parity bit. A label word has a 3-bit-time high-low synchronization pattern and a data word has the inverse 3-bit-time low-high pattern. A message is composed of one to 16 word strings. Each word string has a label word followed by up to 256 data words. The bus can operate in any of the configurations used in MIL-STD-1553 at a 2 Mbit/s rate.

Any one of three media can be used with the ARINC 629 data bus: shielded wire, unshielded wire, or fiber-optic cable. Three modes of bus coupling are possible: current mode, voltage mode, and fiber-optic coupling. However, equipment can communicate on only one of the selected media for a given application.

One noteworthy feature of the 629 bus is the ease of connecting to the bus using an inductive coupler. Figure 4-1 shows an inductive coupler for use in remote or line replaceable unit (LRU) applications. A substantial contribution to improved reliability and reduced electromagnetic interference (EMI) effects is achieved by not having to cut the media wire to make a connection.

Because ARINC 629 is an autonomous terminal access bus, it is necessary for each bus terminal to contain its own control. This control is provided within two erasable programmable read-only memories (EPROMs) that provide transmit and receive functions. The transmit EPROM contains the logic to determine if three conditions have been met before enabling the transmitter. The receive EPROM selects only those messages intended for the terminal and acts as a monitor on the transmitter to guard against babbling and other transmitter malfunctions.

4.2.2.4 ARINC 429: Data Bus—There are cases where it is practical to use the ARINC 429 data bus to transfer digital information to the IMA, such as from areas of low data concentration in the airplane. For example, sensor data could be digitized at the probe and broadcast in ARINC 429 to a central processing location. ARINC Specification 429, Mark 33 Digital Information Transfer System (DITS), describes the details of the ARINC 429 bus.

Aeronautical Radio, Inc. Specification 429 Digital Information Transfer System, Mark 33, 429 is the most commonly used data bus standard in commercial aircraft. It is also the basis for digital buses in modern civil air transports.

Certification requirements on civil transports drove 429 to operate on either 12 to 14.5 KHz or 100 KHz on an unidirectional bus (a unidirectional bus has only one transmitter but has multiple receivers, up to a maximum of 20 for ARINC 429). Communications on 429 buses are either low speed (70 to 93 ms) or high speed (7.5 to 12.5 ms). The low speed is used for general-purpose, low-criticality applications, and a high-speed bus is used for transmitting large quantities of data or flight critical information.

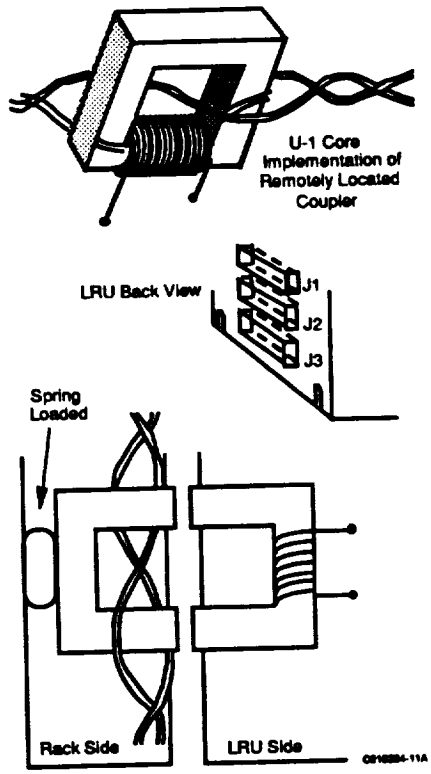


Figure 4-1. Electromagnetic Coupler for LRU Applications

ARINC 429 imposes relatively modest and achievable performance demands on the hardware. The cable used in 429 buses is a twisted, shielded pair of 20 to 26 gauge conductors. The shield is grounded at both ends of the cable run and at all production breaks. Although there is no specification placed on the cable impedance by the manufacturers, it generally falls in the range of 60 to 80 Ω.

4.2.2.5 ARINC 636: Onboard Local Area Network—ARINC Specification 636 was developed in anticipation of high data throughput needs for communications data. This standard is based on the Fiber Distributed Data Interface (FDDI) standard developed for office automation products. It is useful for systems requiring high bandwidth in non-critical applications. (Note: At the time of this writing, the Data Bus Subcommittee is developing these standards.)

The FDDI (ANSI X3T9) standard provides a high-bandwidth, general-purpose interconnection between computers and peripheral equipment using fiber optics as the trans-

mission medium. The FDDI is based on the token ring architecture, whereby a set of stations is logically connected as a serial string of stations and transmission media to form a closed loop. Information is transmitted on the FDDI ring in frames. Messages in packets of up to 4500 octets in size can be sent from one station to another. A timed token rotation (TTR) priority scheme is used to control access to the bus. A point-to-point clocking mechanism is used with the clock being derived at the code-bit frequency (125 MHz) from the incoming pulse stream.

The data are encoded using a 4B5B substitution code, e.g., a 4-bit data is converted into a 5-bit symbol. This is used so that the synchronizing clock information can be recovered from any given series of data bits and to ensure that DC balance can be maintained to the degree feasible to facilitate interface component and circuit designs. Data is transmitted using NRZI modulation, where a polarity transition represents a logical 1 and the absence of a polarity transition denotes a logical 0. With a 125-Mbaud modulation rate, an effective 100-Mbit/s data rate can be achieved. The FDDI can be configured to support a sustained data throughput of approximately 80 to 90 Mbit/s.

FDDI was originally proposed as a packet switching network with two primary areas of applications: first, as a high-performance interconnection between mainframes and their mass storage subsystems and other peripheral equipment, and second, as a backbone network for use with lower speed LANs.

An enhancement to FDDI called FDDI-II adds a circuit switching capability and thus expands the field application to include those requiring the integration of voice, video and sensor data streams.

The basic building block of an FDDI network is a physical connection. This consists of the physical layers of two stations that are connected over the transmission medium by a primary and a secondary link. This is particularly suitable for implementing a dual counterrotating ring configuration. If only one bus is active at a time, the other one can serve as a standby to provide redundancy and reconfigurability. If dual access is selected, then concurrent transmission can be implemented. Other possible FDDI topologies include multiple rings, star, and tree configurations.

An error detection scheme is used to ensure the reliability of the message transmitted. The dual counter-rotating ring concept will enable the FDDI system to be reconfigurable if one or both links between two stations is faulty. A station bypass switch with the capability to bypass any station as specified is used to solve the problem of known broken or powered-down stations. Counterrotating ring connections are required of all stations directly attached in the ring. If a station or link fails, the two rings are folded into one ring, maintaining full connectivity.

Up to 500 stations (1000 physical connections) can be accommodated in an FDDI network, and a total fiber path length of 200 km can be supported. The maximum station separation can be up to 2 km.

The FDDI local area network (LAN) standard is being incorporated into the electronic library and cabin management portions of the Boeing 777 airplane avionics. FDDI is being selected by the ARINC Onboard LAN task group of the Data Bus Subcommittee, which is responsible for LAN standards.

The FDDI data bus was developed for use on Space Station Freedom by a joint effort of Honeywell's Space and Strategic Systems Operations (SASSO) in Clearwater, Florida, and its Sensors and Systems Development Center (SSDC) in Minneapolis. This data bus will carry all the data required to control the environmental and attitude functions of the space station. The FDDI technology represents COTS technology in transition to space applications.

4.2.3 ARINC 638: OSI Upper Layers

ARINC Specification 638 defines the session, presentation, and application layer protocols for aeronautical data communication. (Note: At the time of this draft, the Data Link (DLK) Subcommittee is developing these standards.)

4.2.4 ARINC 637: Internetworking

ARINC Specification 637 defines protocols and addressing definitions for network servicing in the aeronautical telecommunication network (ATN). (Note: At the time of this draft, the data link is developing these standards.)

4.2.5 ARINC 652: Software Management

Software management and the recommendations of ARINC Report 652 are expected to ensure that the software developed for IMA hardware complies with airline desires. Airlines desire modular programs that are easily maintained without prohibitive post-development support costs. ARINC Report 652 also describes the desires of the airlines with respect to software modification and software re-use. (Note: At the time of this report, the Software Management (SWM) Subcommittee is developing software standards.)

4.2.6 ARINC 653: Application Software Interface

A standardized application software environment is part of the commercial IMA concept. ARINC Specification 653 defines an interface standard between the executive soft-

ware and application software. ARINC 653 defines the communication services and memory management facilities expected to be used in avionics equipment ranging from flight control to electronic libraries. (Note: At the time of this report, the APEX Working Group is developing this standard.)

4.2.7 ARINC 624: Onboard Maintenance System

ARINC Report 624 is a design guide for onboard maintenance systems (OMS) used within the IMA maintenance systems. The OMS design guide discusses a variety of maintenance concepts such as BITE, BITE access, and aircraft conditioning monitoring systems (ACMS). The document recommends an English-based user interface, nonvolatile BITE storage and onboard maintenance documentation (OMD).

4.2.8 ARINC 650: Packaging Concepts

The physical parameters associated with the IMA hardware components are described by "form and fit" characteristics documented in ARINC Specification 650, Integrated Modular Avionics Packaging and Interfaces. ARINC Specification 650 specifies cabinet and module dimensions, standardized connectors, environmental criteria and associated parameters that ensure physical interchangeability of modular components. (Note: At the time of this report, the New Installation Concepts (NIC) Subcommittee is developing packaging standards.)

4.2.9 Project Paper 167: Certification and Configuration Control

ARINC Project Paper 617, Guidance and Avionics Certification and Configuration Control, describes procedures used by the industry for certification and configuration control. It also provides recommendations for improving these procedures as evolutionary improvements in avionics occur. Section 7 of this document provides general guidelines that apply to IMA. ARINC Project Paper 617 exists in draft form.

4.2.10 ARINC 613: Ada

The Ada high-order programming language standard developed by the United States Department of Defense (DoD) as ANSI-MIL-STD-1815A is recommended for use in IMA. Ada is the preferred programming language of the airline community. Therefore, it is recommended that all digital avionics be programmed in Ada. ARINC Report 613, Guidance for Using the Ada Programming Language in Avionics Systems, provides recommendations for software engineers using Ada in avionics designs.

4.2.11 ARINC 610: Flight Simulator Avionics

ARINC Report 610, Guidance for Design and Integration of Aircraft Avionics Equipment in Simulators, addresses the use of avionics equipment in flight training devices and flight simulators. Accordingly, where appropriate, the recommendations of ARINC Report 610 should be considered in the design of IMA. Simulator operators and simulator manufacturers should be consulted early in IMA development to determine the additional functions necessary for applying IMA to flight training devices and flight simulators.

4.2.12 ARINC 609: Electric Power

The IMA concept defines a standardized power supply architecture for distributing power in the most cost-effective and weight-saving manner. In designing power supplies with higher criticalities than that of the past and greater emphasis on weight and volume reductions, it is essential that recommendation practices be followed. ARINC Report 609, "Design Guidance for Aircraft Electrical Power Systems," describes airline and industry concerns and acceptable standards.

4.2.13 Related Documents

EUROCAE ED-14x—Environmental Conditions and Test Procedures for Airborne Equipment (future revision).

EUROCAE ED-12x—Software Considerations in Airborne Systems and Equipment Certification (future revision).

RTCA DO-160x—Environmental Conditions and Test Procedures for Airborne Equipment (future revision).

RTCA DO-178x—Software considerations in Airborne Systems and Equipment Certification (future revision).

RTCA DO-205—Design Guidance and Recommended Standards to Support Open Systems Interconnection for Aeronautical Mobile Digital Communications.

4.3 System Architecture

4.3.1 Introduction

This subsection examines the characteristics and attributes of commercial aircraft architecture and subsequently provides examples of COTS+ architectures using commercial, ruggedized, and militarized technology. Candidate configu-

rations are described, and issues governing the desirability of each configuration are discussed in the context of performance and dependability. A point-of-departure, strawman architecture is used within this study as an example from which further assessments and comparisons to other configurations can be made. The strawman architecture incorporates the Boeing 777 airplane's Aircraft Information Management System (AIMS) architecture and several other COTS+ technologies described within the Standard Modules section of this report. This subsection relates only to architectural hardware components and design configurations. Further definition of COTS+ architecture, including system-level rules governing the full or partial use of COTS+ hardware, software, requirements, interconnections, and the developmental support resources required to implement designs are discussed elsewhere within this document.

COTS+ systems are likely to be in existence for a long time, during which there will be many technological developments that can improve architectural designs. These developments are likely to occur at different times for different components, which places a requirement on the system to be able to accommodate these different technologies. This can be achieved through careful definition of architectural element boundaries and by ensuring that the elements are loosely coupled to each other.

Data interface standards ARINC 629 and ARINC 659 have been developed to positively influence equipment interoperability. This enables equipment to be specified, constructed, and qualified independently from the remainder of the system, yet function with other modules in the system following integration.

The focus of this subsection is guidance for the implementation of a COTS+ systems architecture. As such, it is concerned with the definition of components that lend themselves to standardization. It is, therefore, not concerned with component (sensor, actuator, or indicator) design details except for interfaces to other components.

4.3.2 IMA Derived COTS+ Architecture

4.3.2.1 Distributed Architecture—

Commercial Approach to Functional Distribution—The commercial aircraft IMA architectural approach promotes the use of logical systems, or more importantly, concentrates functions without constraints imposed by physical boundaries. This allows sensors, actuators, indicators and processors to be shared by many functions.

The commercial IMA system architecture can, therefore, functionally accommodate many current aircraft systems and may ultimately include them all. Figure 4-2 gives an example of functional distribution. This figure illustrates the diversity of functions that can be handled by any one cabinet in an aircraft system. Functions are shown as being allocated to a specific cabinet. Because functions generally need sensor information and usually provide an output to either an indicator or actuator or both, they must be connected in some way to the devices. These devices are rarely collocated with the cabinet, and in general, require many wires to perform their function. Where the sensors, actuators, or indicators are distantly located from the cabinets, commercial IMA architecture provides benefits by incorporating electronics that convert source/sink data into digital form so they may be connected directly to a serial bus. Besides enabling the designer to maximize the potential for weight saving by minimizing discrete wiring, this approach improves the maintainability of the system because the vehicle's wiring can now be monitored in situ by more than one component.

COTS+ Approach to Functional Distribution—The COTS+ space vehicle architecture uses the commercial IMA architectural approach with the exception that it is greatly influenced by physical restrictions that are imposed by manufacturing partitioning and required to improve space vehicle performance and fault tolerance. These differences and their influences are explained as follows:

1. COTS+ architecture must accommodate physical restrictions imposed by the fabrication of space vehicles. Some functions such as sensor buses may be separated and included within different subsystems because vehicle stages are physically separated by stage size or to facilitate manufacturing and/or fabrication operations.

2. The COTS+ approach is distinguished by its use of physical boundaries and partitioning to promote the use of NDI equipment qualified to operate under commercial environments. COTS+ requirements may require installations within environmentally protected areas or within areas with less harsh environments to ensure avionic performance and fault tolerance.

By adapting the functional distribution approach promoted by commercial IMA architecture, it is possible to concentrate functions and install processing hardware, for instance, at remote locations within the space vehicle structure away from their associated sensor sources and effectors. These locations, selected because of their favorable physical environments may be characterized by lower levels of vibration and/or acoustic noise, less susceptibility to shock, lower radiation levels, less susceptibility to electromagnetic environment (EME), and less effect from outside temperature extremes.

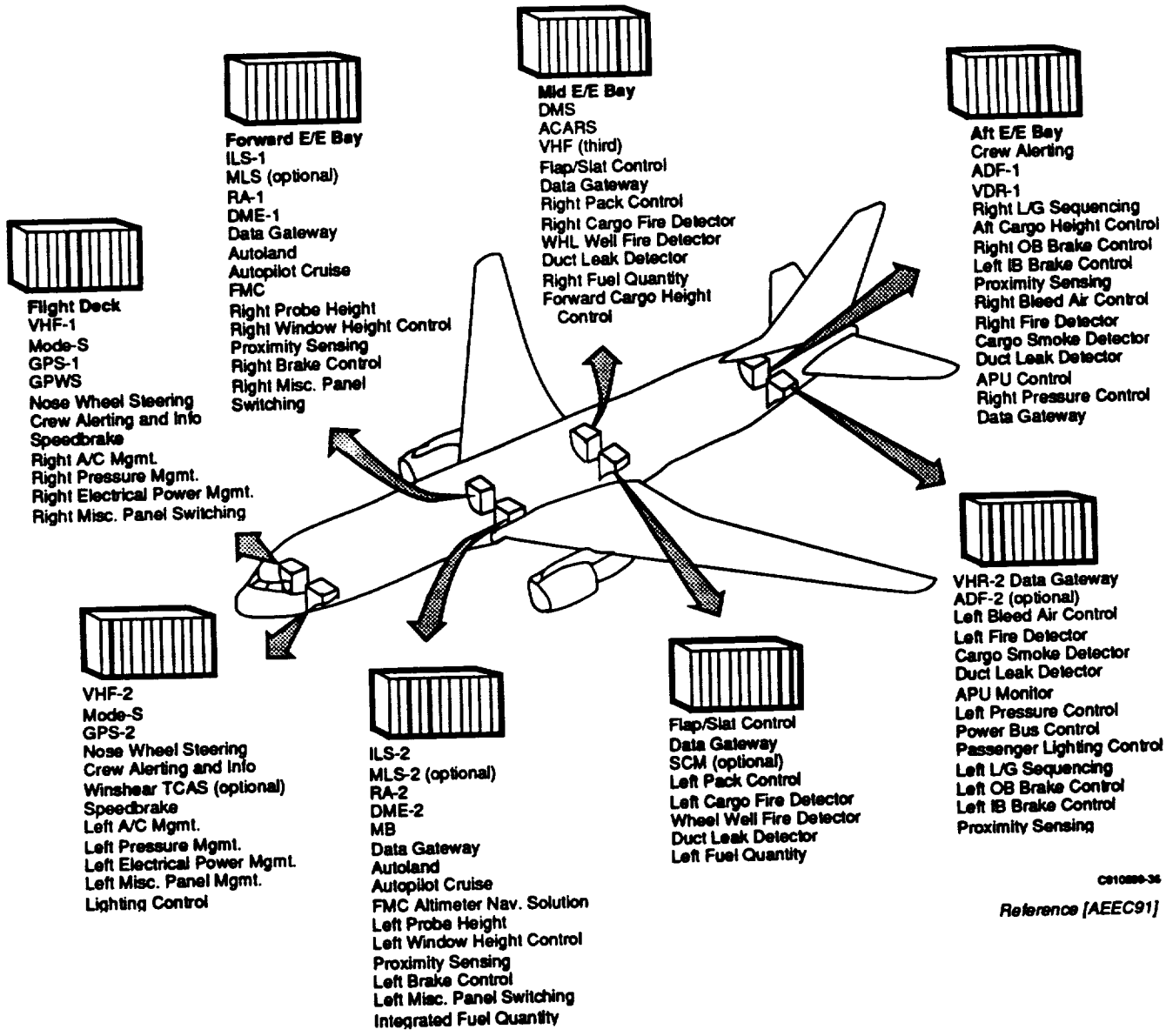


Figure 4-2. Functional Description Example

A functionally distributed COTS+ space-vehicle architecture is illustrated in Figure 4-3. The figure shows two examples of functional distribution that accommodate physical restrictions imposed by manufacturing partitioning, performance, and fault tolerance. Engine controllers are located at remote locations, allowing controller avionics to be qualified to lower environmental levels. For a given design, operation within more benign environments assures higher levels of performance (dependability and fault tolerance). The figure illustrates remote engine control processors removed an appreciable distance away from the harsh engine environments. Illustrations are shown for a manned and an unmanned vehicle. Engine controllers installed within radiation-protected, controlled cabin environments are illustrated for the manned vehicle.

Sensor and effector interfaces are provided through remote data interface (RDI) units. The RDI concentrates sensor and effector signals/commands, provides signal control and conditioning, and provides a standard interface to the vehicle's data network. The RDI's standard network interface is essential to the manufacturing partitioning of the engine module, since it provides a network interface necessary for independent testing of the engine module and establishes an interface requiring minimum connections.

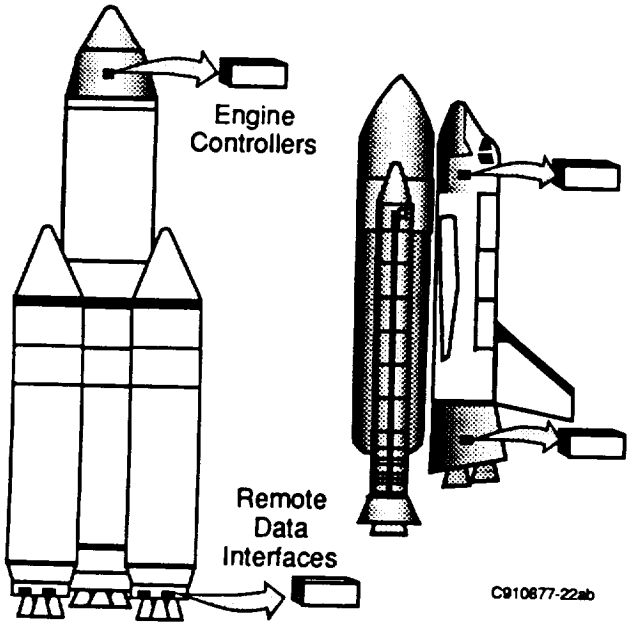


Figure 4-3. Functionally Distributed COTS+ Space Vehicle Architecture

Although the distributed architecture philosophy allows processor electronics to operate within less harsh environments, the RDIs in the above illustration are required to operate at harsher environmental levels. For this example, provisions would be provided for RDI operation within the engine environment; that is, they would have to be either ruggedized, militarized, or modified to the spacecraft environment; or, by default, be replaced by space-qualified RDIs designed specifically to withstand environments near engines.

4.3.2.2 Physical Distribution—

Commercial Aircraft IMA Equipment Distribution— Commercial IMA equipment is distributed throughout the aircraft in a way that minimizes the aircraft's life-cycle costs. Three primary types of equipment are considered: cabinets, LRUs and remote components.

Commercial aircraft IMA cabinet locations can be established after analyzing the tradeoffs of the convenience of the location versus proximity to sensors/actuators. Cabinet I/O requirements may be affected by the choice of cabinet location. Proper equipment location results in saving wire lengths, connectors and manufacturing costs. Tasks that are strictly performed in software could be run in a cabinet in any location in the aircraft. It also is practical to have one cabinet provide the I/O for nearby sensors and supply the data over ARINC 629 buses to another cabinet. This approach can significantly reduce the wiring for systems that are spread throughout the airplane.

In cabinets containing gateways as their only I/O (i.e., they do not interface to sensors/effectors), the cabinet is relatively insensitive to location and can be placed wherever it is most convenient to the maintenance personnel. Certain applications with different cost drivers may result in other I/O line-replaceable modules (LRMs) located in the cabinet. In such cases, the wiring associated with the I/O can place restrictions on the cabinet location, and the cabinet must be placed in a location that minimizes the airframe wiring task.

Remote electronics are incorporated in the relevant device where this is a practical solution, such as smart sensors and actuators with intelligent bus/network interfaces. Other devices may be handled by remote data concentrators that service a number of physically close devices. Remote data concentrators are located at points convenient to the devices and the maintenance personnel. Where neither of the above options is possible, the I/O should be placed in the cabinet.

COTS Space Vehicle Equipment Distribution— COTS+ space vehicle equipment, like commercial aircraft IMA equipment, is distributed throughout the space vehicle in a way that minimizes the vehicle's life-cycle costs. COTS+ equipment, however, is first partitioned to reside within physical and geographical boundaries established to facilitate commercial equipment operation within commercially defined environments. Within the physical boundaries established by partitioning, cabinet and remote unit locations are established after analyzing the tradeoffs of the convenience of the location versus proximity to sensors/actuators, and so on, as with IMA distribution analysis.

The three primary types of commercial IMA equipment—cabinets, LRUs, and remote components—are also the principal components used in the COTS+ space vehicle architecture. Incorporation of unaltered IMA equipment within the COTS+ architecture maximizes the use of commercial off-the-shelf subsystems.

4.3.3 System Components

The components normally required to implement a space vehicle avionic function are controls, sensors, actuators, indicators and the processing necessary to transform data into a form suitable for driving actuators and indicators. The COTS+ architecture treats these components as separate physical entities that communicate with one another via a network of data buses. The COTS+ architecture aims to reduce costs by optimizing the location of the processing of many functions.

The components of a COTS+ architecture include:

- Cabinets;
- Data buses (ARINC 629, ARINC 429, FDDI, Taxi);
- ARINC 629-compatible devices;
- Peripherals that are directly connected to cabinet;
- Data concentrators.

These modules should be interchangeable and should work together. Therefore, a rigorous definition of the static aspects of the interface are necessary. This includes connector definition, pin-out, and signal characteristics. The level of redundancy provided as part of the fault-tolerant aspects of the cabinet affects interchangeability. Therefore, the level of redundancy needs to be defined to ensure that each implementation conforms to the same standard.

For the systems that are implemented in the COTS+ cabinet to meet their integrity requirements, the cabinet may need to provide a means for incorporating dissimilarity. This dissimilarity may be needed at the software or hardware level or both. A high degree of integrity is recommended for all COTS+ equipment.

The remainder of this subsection describes the components in more detail. Previously described components are described within the context of system architecture.

4.3.3.1 Cabinet—The purpose of the cabinet is to provide the computing resources and interfaces necessary for all application software that resides in the cabinet. The cabinet may also house I/O for local devices. A commercial off-the-shelf airplane cabinet is illustrated in Figure 4-4.

Three prime elements are considered to be part of the cabinet: the cabinet frame, the functional modules, and the backplane bus.

Cabinet Frame and Backplane Assembly—The cabinet frame provides the mechanical and electrical environment for installing a group of functional modules and forms the interface between the modules and the airframe. The overall dimensions of the cabinet are flexible so manufacturers can integrate a variety of modules into a particular airframe. Cabinet designs are likely to be unique so they can withstand different environments. This allows maximum flexibility in locating cabinets in the airframe.

The cabinet also contains the physical backplane that performs the interface between functional modules and the rest of the avionics. The backplane can be divided into three areas. The first area interfaces vehicle wiring to the physical backplane. The second area is dedicated to the transfer of all intermodule traffic, i.e., backplane buses and module interconnections. The third area is used for power distribution. The ARINC 659 backplane bus is an important functional element of the cabinet.

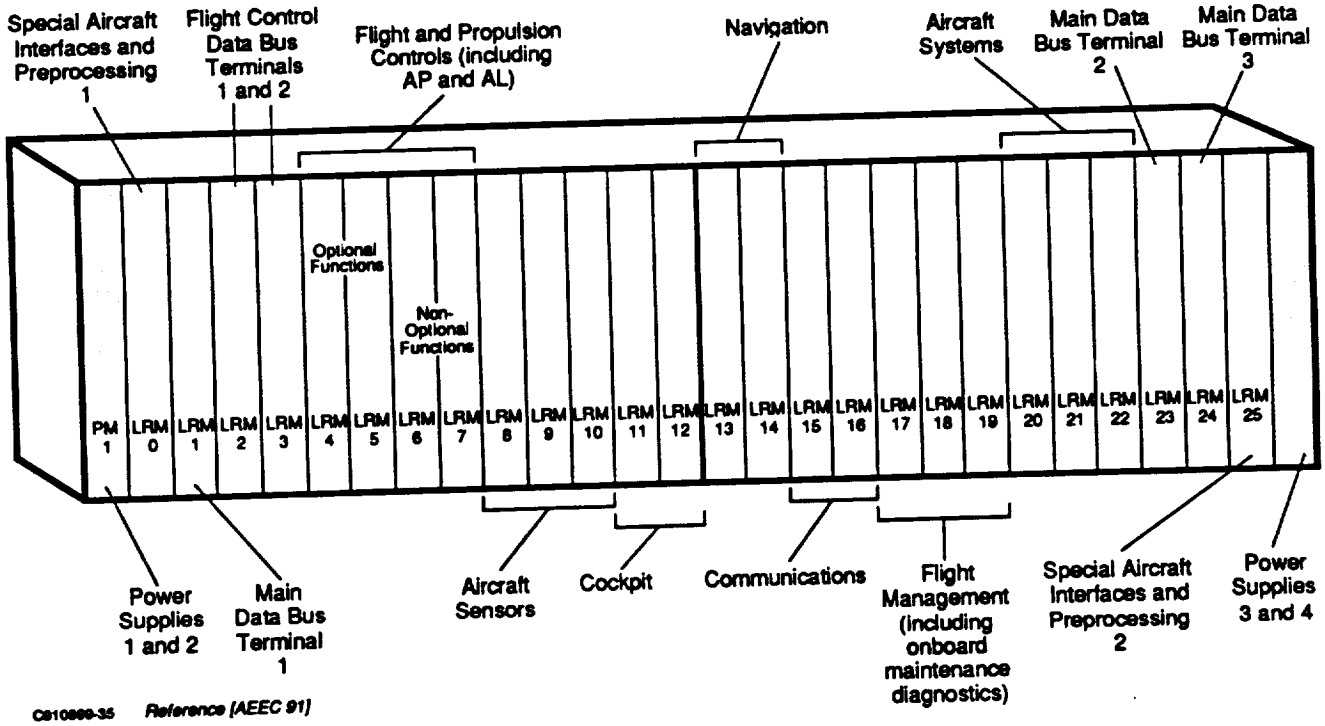


Figure 4-4. COTS Airplane Cabinet

Cabinet Design—The cabinet design is the responsibility of the system integrator, the vehicle manufacturer. Each cabinet shall provide a fault-tolerant environment. Functions are distributed in cabinets based on the need for I/O, data throughput and memory requirements as well as their relationship with other functions. The cabinet conforms to the appropriate sections of ARINC Specification 650 and RTCA Document DO-160 standards.

The cabinet itself provides the basic mechanical structure and environmental control/isolation for the modules. It does not provide any electrical services such as power transformation/regulation and bus control/monitoring. Individual LRMs provide these services for the avionics functions.

Several cabinet designs are to be defined to withstand different vehicle environments while allowing the LRMs to be designed to a single environmental specification. The cabinets are to be of open or closed construction to allow maximum flexibility in locating them with respect to fluids, particles, high-intensity radiated fields (HIRF), etc. Different cabinets shall use the same modules. Additional maintenance procedures caused by different cabinet styles shall be minimized.

ARINC Specification 650, Integrated Modular Avionics Packaging and Interfaces, defines the physical and environmental characteristics of the cabinet. A general view of a cabinet assembly is shown in Figure 4-5.

4.3.3.2 Line Replaceable Modules (LRMs)—The functional modules are packaged as LRMs. The ultimate aim of COTS+ IMA is that the vehicle interfaces are either common to most modules or configurable so that the number of modules and their position in the cabinet need not be fixed during vehicle design but may allow modification and addition of functions, in service, without costly changes to the cabinet and vehicle wiring.

Several modules have been defined for the COTS+ architecture, including:

- Core processor,
- Standard I/O,
- Special I/O,
- Power supply module,
- Bus bridge,
- Gateway.

The function of each module and the definition of its interface to the backplane is specified in separate ARINC characteristics. This approach is intended to ensure interoperability of equipment designed and installed by different manufacturers. It also promotes the objective of equipment interchangeability. When modularity is achieved, it will result in avionic systems that are easy to develop, certify, test, and maintain.

The level of redundancy provided internally is determined by the implementer of the module and reflects the requirements of the program. The system integrator shall assess the capabilities of the module against the system requirements and make the selection accordingly.

The LRM connector definition and pin-outs are to be standardized to conform to ARINC Specification 650, Integrated Modular Avionics Packaging and Interfaces.

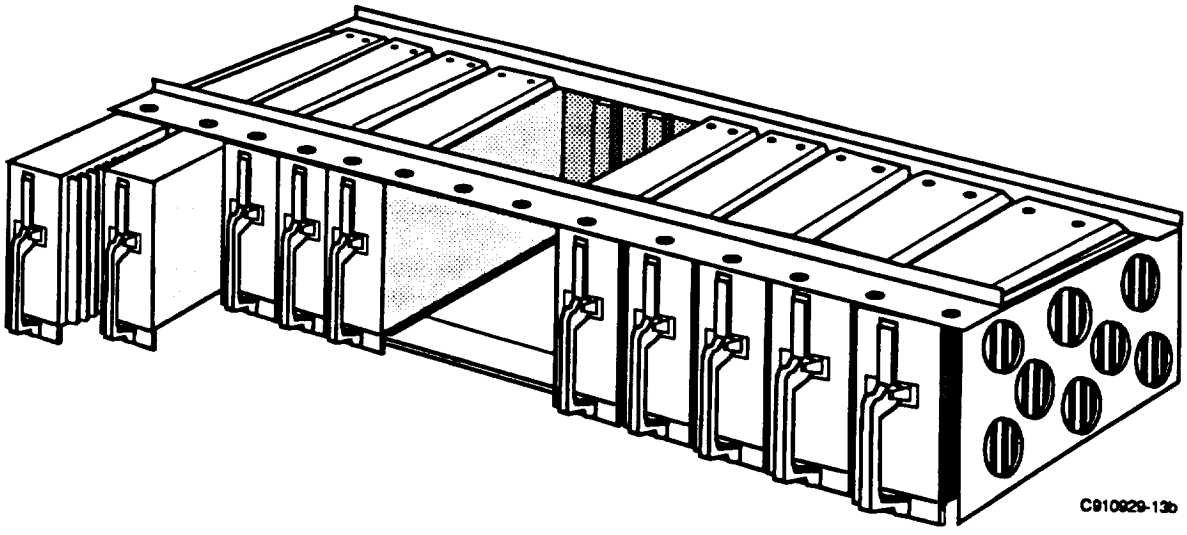


Figure 4-5. General View of Cabinet Assembly

Core Processors—The core processor provides the computing power for the cabinet. The cabinet may contain one or a number of processors together with their memory and any circuitry necessary for redundancy management, such as monitors, BITE, and isolation circuits. In the COTS+ IMA concept, alternate core module designs may be based on the cabinet applications.

Because the core processor must run many different functions, it must provide a means of protecting the functions to ensure that no one function can adversely affect another. The means of isolation should be invisible to the application software.

Each system implementation will determine how many processors and how many different designs should be used. The design of a core processor shall promote implementation independence to allow true interchangeability with any other core in the cabinet, concurrence between other cores in the cabinet, and concurrence between suppliers.

Application software may be loaded in any of the core processors within a cabinet, the design of which should allow transparency of hardware support for the applications.

Consideration should be given to using hardware to support specific executive aspects such as:

- Partitioning for memory and time allocation,
- Privileged access to avoid interference between applications,
- Redundancy management of the core or cabinet.

Data Bus Interfaces—A gateway module converts data from vehicle bus format to the format required by the backplane bus (intercabinet and intracabinet buses, respectively), to allow the distribution of data from the vehicle to the cabinet modules and vice versa.

It is possible for a data gateway to provide data transformation service for the cabinet. The use of a separate gateway isolates the bus technology and protocols from the remainder of the cabinet. Bus bridges may be used to transfer data to and from data buses of the same type. All hardware necessary to implement the gateway and the related software should reside in the gateway module.

Although the primary COTS+ data bus is ARINC 629, other networks and buses, such as the ARINC 429, FDDI, and Taxi data buses, shall be accommodated. Therefore, a family of bus bridge modules and gateways will be developed to cover different mixes of bus standards and different capabilities.

The COTS+ system designer shall consider the full complement of data bus interfaces to the cabinet. To cope with possible evolutions of cabinet functionality or the module technology, gateways should be used to convert protocols from different data buses. A typical gateway would convert the ARINC 629 global bus protocol to the ARINC 659 backplane bus protocol and vice versa.

If a gateway may be the sole interface between the cabinet and other aircraft systems, its design should take into account the safety and availability requirements of the entire system.

The gateway shall take into consideration the recommendations of the OSI Reference Model. This concept is aimed at providing the module with the desired level of flexibility. Gateways should be configurable and contain some processing capability.

Repeaters, bridges, and routers are other data bus interface techniques that shall be considered in system design. Subsection 4.4, describing data networks, provides additional background material.

I/O Modules—A family of LRMs will be developed to transform a standard set of analog and discrete sensor data types into digital data to be transferred to the core processors via the backplane bus or vice versa. Each LRM may contain interfaces to a single type of signal or to some optimum mix of signals.

Standardization of I/O modules will promote efficient acquisition of data to be transmitted to the processing modules via the backplane bus. The standardization of an individual I/O module should consider the means for reconfiguration. The I/O module can be configured by the application software to meet the cabinet requirements, and this configuration can be stored in the I/O module memory.

Where special signal types or interface requirements cannot be met with a standard I/O LRM, it may be necessary to develop a special LRM. This should be done only where absolutely necessary, because the cost advantage of standardization may not be realized. System engineering should be used to minimize the various types of signals that require special I/O LRMs.

The definitions of the standard I/O modules are provided in Subsection 4.1, Standard I/O Module. Descriptions of synchronous and asynchronous aspects of I/O modules follow.

Synchronous I/O Modules—Synchronous I/O modules exchange data between the I/O module and the core processing modules as required by the application (i.e., they are synchronous with the application). The module performs data acquisition, preprocessing and block storage according to the requirements of the applications present in the cabinet.

Each application configures the I/O for its own use immediately after the determination of the cabinet configuration. After this, the preprocessing unit should cyclically refresh the memory allocated to each application. The same data can thus be found in the memory of the I/O modules in the areas specific to the application.

Asynchronous I/O Modules—In the asynchronous mode of operation, the exchanges between the I/O module and the core processing modules are left to the initiative of the I/O module. These transmissions are asynchronous with respect to the application. These modules provide data acquisition, preprocessing, and block storage functions to the various applications present in the cabinet.

When the cabinet configuration has been determined, each application can inform the I/O module of the signal characteristics it requires—the type of signal, the electrical value-physical value conversion, the signal refresh rates on the backplane. After the module has been configured and initialized, it should transmit all its acquisitions to the appropriate modules.

In both synchronous and asynchronous modes the preprocessing unit should be capable of processing the data. In addition, it should be capable of acquiring and storing I/O signals. The characteristics of the processing should be loaded in the same way as the channel characteristics.

Power Supply LRMs—For modular architectures, the power supply LRM provides power to other modules. The power supply LRM provides power isolation and conversion between vehicles power requirements of other LRMs (user modules). The set of supply modules in each cabinet should have redundancy commensurate with the integrity requirements of the functions executed in the cabinet.

Two independent sources of standard Vehicle power provide input power to each supply module in a cabinet. Output power from a supply moduleis a conditioned voltage level. The supply modules should provide separate output lines for each connected user module. These output lines should have independent fault protection so that a fault in one user module does not affect the integrity of the power supplied to the other user modules.

User modules are normally connected to at least two supply modules. Each user module automatically draws power from either (or both) of the supplies as required to accomplish the module's functions.

Design guidance for power supply modules is contained in Subsection 4.1.

4.3.3.3 Backplane Bus—The ARINC 659 serial data bus is used for intermodule communication. A serial backplane data bus has many advantages compared with a parallel bus, including minimal pin count and associated interconnections inside the cabinet. It also provides exceptional architectural flexibility for high criticality systems that require multiple backplane buses to meet the integrity goals.

4.3.3.4 Test and Maintenance Bus—A separate data bus is recommended for the purpose of uploading ARINC 659 software tables. The recommended data bus is specified in IEEE Standard 1149.5.

4.3.3.5 Vehicle Data Bus—The primary vehicle data bus is ARINC 629 defined in ARINC Specification 629, Multi-transmitter Data Bus, Part 1 - Technical Description. ARINC 629 serves as a global resource and should be used to transfer all data between cabinets. In addition, ARINC 429 and other networks can be used for particular applications where it is appropriate.

The ARINC 629 data bus is a serial bidirectional data bus used to transmit all data including critical data. The overall system requirements determine the number of buses needed for a specific implementation. Initially, buses should be designed to operate at no more than 50% of capacity, thereby allowing sufficient growth margin. In cases where the data path is specialized or high traffic volumes are anticipated, such as structured OSI communications, dedicated ARINC 629 buses should be used.

4.3.3.6 ARINC 629-Compatible Devices—Interfaces to the outside world (sensors, actuators and indicators) may contain remote electronics to perform signal conditioning buffering, conversion, and low-level control. The remote electronics can be incorporated in devices such as an air data probe where there is a practical solution. Such devices include ARINC 629 compatible actuators and sensors.

Other devices not compatible with ARINC 629 can use remote data concentrators that service a number of devices in proximity. Data concentrators convert device data into digital form, which is transmitted on the ARINC 629 data bus. In the receive mode, they convert digital data into analog form. The remote devices are responsible for conditioning the data from the concentrators under their control and for monitoring the health of the sensors/actuators and any circuitry within themselves. This approach has the advantage of minimizing the number of discrete wires in the aircraft.

The COTS+ architecture encourages the development of ARINC 629-compatible devices, since they enable a

greater degree of system implementation and freedom of modification. The maintainability of systems also is increased because vehicle wiring can be monitored and, because the bus is a multiaccess bus, it can be monitored at more than one point.

4.3.3.7 Simple Devices—Peripherals, incapable of being directly connected to the ARINC 629 data bus, are referred to as simple devices. This implies nothing about the internal sophistication of the devices. Simple devices may output raw data or may have complex internal processing to perform signal conditioning, buffering, conversion, and low-level control. Their data output may be in analog form or in digital form other than ARINC 629. It is recommended that simple devices interface to data concentrators for transmission on the ARINC 629 bus or interface directly to cabinets through standard I/O modules.

When special signal types are present or special interface requirements cannot be met, vehicle-specific devices must be designed. This should be done only when there is no other practical solution. If the reason is cost-effectiveness, the total vehicle and program cost should be considered, not just the cost of the device.

4.3.3.8 Display Devices—Generally, ARINC 629 data buses are used to interface display devices. However, some display architectures and economic tradeoffs result in attractive alternatives. For example, some display devices may be connected to the cabinets via high-speed video buses. This type of interface would be necessary if the cabinet designer elects to integrate the display graphics generation into the cabinet hardware and transmit video data to the display devices.

Several issues should be considered when assessing the desirability for a high-speed video interface. System designers should consider the users' desire for increased equipment reliability. Minimizing the complexity of display devices will improve the cabin equipment reliability. This improvement typically will require increased bandwidth between the cabinets and the display devices. Other design issues to be considered include reducing the number of part numbers, reducing flight deck power distribution, and increasing availability through multiple reconfiguration paths.

4.3.3.9 Remote Data Concentrators—A remote data concentrator serves a number of simple devices in close proximity. It converts source data from simple devices into digital form, which is transmitted on the ARINC 629 data bus. It accepts analog, discrete, RF, etc., data in the form suitable to the device. The data concentrator can be responsible for monitoring the health of simple devices or sensors.

When it is impractical to interface simple devices directly to the COTS+ cabinet, remote data concentrators should be used to the greatest extent possible. Remote data concentrators are defined in Subsection 4.7, Data Sources and Destinations.

4.3.4 High-Integrity Design Requirements

A basic goal of commercial COTS+ IMA is to develop an architecture that meets dependability and safety requirements. Depending on the architecture, the approach to integration, and the number of systems being integrated, some level of fault tolerance will be necessary to meet the requirements.

High-integrity COTS+ designs are needed to satisfy dependability and safety requirements. In addition, avionics systems must demonstrate high availability, even for systems that are not flight critical. This approach positively contributes to efficient vehicle operation and minimizes opportunity cost losses. As a minimum, fault tolerance is to be applied to all functions that could jeopardize reliable operation. This philosophy drives space system designs and is used as design criteria for determining space system architecture, its level of fault tolerance, and candidate systems for integration.

4.3.5 Candidate COTS+ Architectures

Six commercial off-the-shelf architectures are described in this subsection. They comprise configurations exhibiting different logical, functional, and physical structures. Five architectures are described in ARINC Report 651 and the sixth, Boeing' s 777 avionics architecture, is presented as a design currently being implemented.

The COTS+ architecture defines the physical and logical relationships among the components, their connections, and their functional elements, which include sensors, processors, monitors/displays, and control/actuating devices. The physical relationships are determined by the geographical distribution of functional elements, while the logical relationships are determined by the hierarchy of control for data and signal processing among the various elements. The processing for an element of COTS+ includes its means for controlling and/or being controlled, whether it is implemented in software, firmware, or hardware.

Based on the physical and logical relationships among various elements and components, COTS+ architectures can be classified into several categories. Five categories are presented in ARINC Report 651, Design Guidelines for Integrated Modular Avionics. The architectures, although described individually, are not absolute. It is envisaged that

system requirements may render a hybrid of these architectures to be most effective for some specific applications. The ARINC Report 651 architectures are identified alphabetically from Architecture-A through Architecture-E. Further detail on these architectures is provided in ARINC Report 651.

Boeing' s 777 avionics architecture is an alternate manifestation of commercial concepts and may be considered a hybrid of the ARINC 651 architectures. The 777 architecture contains Honeywell AIMS cabinets and will be used as the baseline architecture of this study.

4.3.5.1 ARINC Architecture-A—Architecture-A connects autonomously operating LRUs in a fashion similar to that established for commercial LRUs (the ARINC 700 series LRUs). Because the architecture is partitioned similarly to traditional avionic architectures, avionic certification requires few innovations compared with established procedures.

Architecture-A employs four cabinets interconnected by quad 629 data buses; all avionic functions are implemented in the four cabinets. Each cabinet uses similar hardware for redundancy. The general architectural outline is shown in Figure 4-6. Each avionic cabinet contains separate data and signal processing capabilities to support different avionic functions simultaneously. LRMs implement different avionics functions. The functional relationship between different LRMs is logically distributed, but each LRM provides logically centralized control with physically distributed architecture.

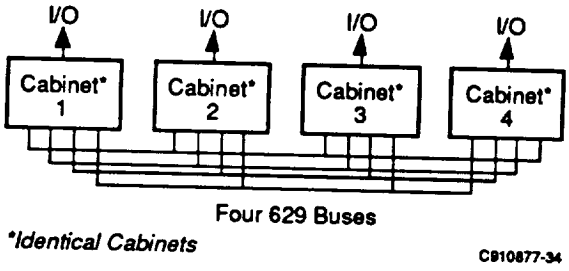


Figure 4-6. Architecture-A

Fault Tolerance Considerations—Each module is to provide a fault-tolerant environment. Each LRM contained in the avionics cabinet has its own fault containment area to ensure that faults can be isolated to an LRM for maintenance purposes.

4.3.5.2 ARINC Architecture-B—Architecture-B is based on a concept of logically centralized processing. The core processor is collocated with the I/O electronics for sensing and control functions. All I/O functions operate under the control of the processor. The main advantage of this architecture is simplicity and analyzability that results when all interface circuits and their operations are under complete control of the processor, which is the logically central control element. The general architectural outline for Architecture-B is shown in Figure 4-7.

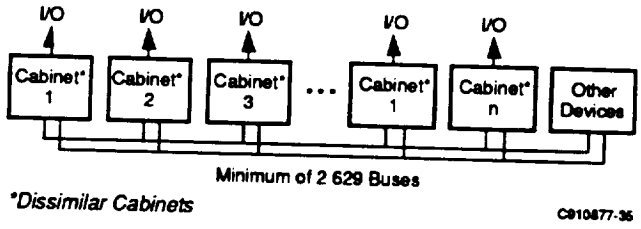


Figure 4-7. Architecture-B

Fault Tolerance Considerations—The key consideration in this architecture is the provision for deterministic operation. The remotely controlled sensors and actuators are designed with interfaces that are fully testable and analyzable. The architecture may employ dissimilar sensors and actuators to reduce the probability of generic errors. This type of architecture lends itself to a relatively straightforward validation procedure.

Functional integrity and availability of the system is achieved by providing a fault-tolerant cabinet environment and also through system-level cabinet redundancy. Cabinet fault tolerance is achieved by implementing fault tolerance at the module level. Core processor module fault tolerance is provided by requiring redundancy of processor components within the module. As a minimum, each fault tolerant module implements a pair of dual-redundant processors. This is analogous to a dual-dual redundancy configuration. Fault tolerance for the cabinet is implemented using similar hardware to provide redundancy, but dissimilar redundancy is implemented by coding the application program in two or more cabinets with different processors.

System-level redundancy is provided through implementing redundant cabinets to further enhance the functional availability and integrity of the system. The number of cabinets is limited to interunit performance limitations only.

At the module level, each module provides its own fault-tolerant environment. This is to ensure that faults can be isolated to an LRM. Maintainability is designed into the cabinet so that all failures causing loss of a function can automatically be isolated to the faulty LRM.

At the backplane level, the backplane data bus provides the capability to detect and isolate bus faults and provides a reconfiguration path around the failure. The backplane bus is implemented in a dual-redundant configuration. The bus

contains error detection and correction capability and has the ability to contain bus faults. There are no single-point bus failure modes that could cause the loss of both buses.

4.3.5.3 ARINC Architecture-C—Architecture-C is logically centralized and physically distributed. A general architectural outline for Architecture-C is shown in Figure 4-8. Each component of this architecture is a virtual node capable of providing autonomous operation in a cooperative manner with other nodes.

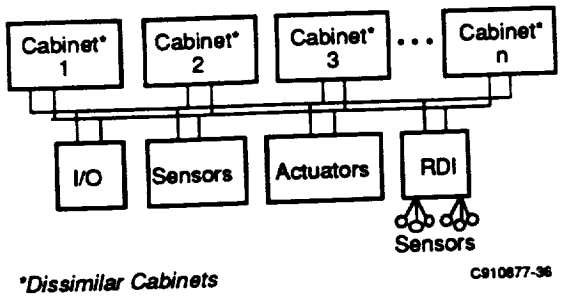


Figure 4-8. Architecture-C

This architecture is based on the physical distribution and separation of functions, while the logical relationship between different functional elements is a hierarchy of control determined by the core processor. The core processor monitors all the I/O interfaces (whether located centrally or remotely), determines the appropriate action, and controls the displays and/or actuator and control mechanisms.

In a preferred configuration, I/O is handled by remote data concentrators located remotely from cabinets, thus physically separating processing functions from their sources of raw data and sinks of processed data. This is especially important to minimize the complexity of system upgrades. Wherever possible, sensors and actuators are also remotely located. They are "smart" in the sense that all inner-loop control functions are located on the devices themselves.

The major difference between Architecture-B and Architecture-C is that processing resources are physically independent of their I/O data in Architecture-C, whereas in Architecture-B they are not, because of the association of both applications functions and their I/O data in the same cabinet.

In Architecture-C, the preferred cabinet external data interface is to the ARINC 629 data bus. All system-level communication between cabinets, sensors, actuators and other devices is via ARINC 629 data buses. However, the architecture does not preclude other forms of cabinet-resident I/O where costs dictate that I/O be located in the cabinet. However, where I/O is located in cabinets, the location independence of applications may be compromised.

Fault Tolerance Considerations—The architecture employs fault detection, fault isolation, and a redundancy management scheme passing active control from failed elements in the network to functioning elements to provide transparent operation.

In Architecture-C, functional availability and integrity are regarded as top-level properties of the avionics suite and can be achieved by the appropriate interconnection of elements that need not in themselves be as fault tolerant as the complete system. Fault tolerance in Architecture-C can be provided by the replication of applications functions onto redundant elements at the system, cabinet, and/or LRM levels. This structure enables dependability to be provided most cost-effectively for the individual elements of avionics functionality. The design of the fault tolerance is implemented in such a way that the system-level disruption and recertification effort because of new application programs, LRMs, or cabinets is minimized. Additionally, because of the separation of applications from their raw data sources, Architecture-C supports the concept of gracefully degrading system operation in the presence of noncritical faults.

System-level redundancy is achieved by the implementation of redundant cabinets where applications are replicated across these redundant cabinets. The cabinets may be dissimilar. The outputs of the replicated applications are used for failure detection and isolation at the system level. System-level redundancy is further enhanced through providing multiple data transfer paths between system elements by means of redundant ARINC 629 data buses.

Cabinet-level fault tolerance is provided through the replication of applications functions across redundant LRMs within a single cabinet. These LRMs may be dissimilar. In Architecture-C, the LRMs need not be fault tolerant since replication at cabinet and/or system level is available.

LRM-level fault tolerance may be provided by the replication of application functions across a single LRM. These applications may be of dissimilar design and implementation but targeted to a common processor.

4.3.5.4 ARINC Architecture-D—Architecture-D provides a flexible, fault-tolerant avionics architecture that can be reconfigured. The architecture is physically and logically distributed. The system architecture is illustrated in Figure 4-9.

Fault Tolerance Considerations—Each cabinet contains fault-tolerant elements to provide redundancy on the module and backplane levels so maintenance actions can be deferred to a scheduled maintenance time and an application may be configured.

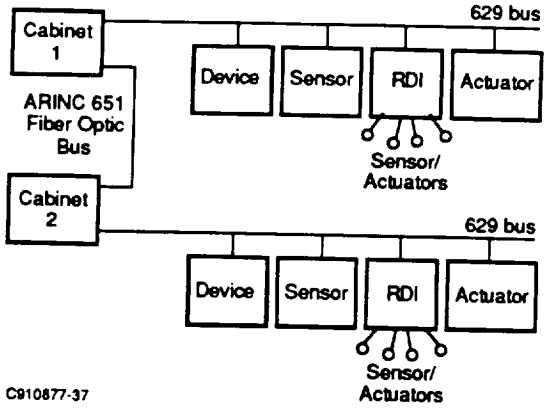


Figure 4-9. Architecture-D

After a failure that affects a certain application, the configuration of applications at the cabinet level must be reorganized so that the affected application can continue to operate properly. This reconfiguration within a cabinet or between cabinets expands the application lifetime ("fit and forget" philosophy).

The avionics applications are distributed in the cabinets based on level of criticality, relationship with other applications, memory/processing power, location of used remote systems, and so on.

In Architecture-D, the level of redundancy is determined by the level of criticality of the application function. It also requires a certain level of redundancy of data buses to be considered, depending on the criticality of the data, to account for integrity of the transferred data.

Fault tolerance can be applied on the cabinet modules, data bus level (multipath possibilities) by reconfiguration within and between cabinets. Reconfiguration within and between the cabinets is employed to defer maintenance actions.

Reconfiguration—Reconfigurability in commercial architectures is used to improve the fault tolerance of the architecture. The components in a logically distributed architecture are able to independently and dynamically control their operation, rather than being dependent on a central element controlling their operation. This allows dynamic reconfigurability in the architecture. In Architecture-D, this feature is used to improve the fault tolerance of the architecture.

The reconfiguration function defers maintenance actions without jeopardizing the safety aspects. This function is part of the executive (core processing module). It uses configuration information from the reconfiguration strategy table, which provides multiple reconfiguration paths to the executive.

In the case of a processing or application module failure, this function attempts to reconfigure the affected applications to other processing modules in the same cabinet or to other cabinets so there is no performance degradation in the system.

This technique may be used to reduce processing module burden. The reconfiguration function can determine via a specific table which applications are needed to fulfill the intended avionics functions at every moment of flight. Not every application has to run simultaneously. For example, there is no need for the wind shear function in the cruise mode of flight.

4.3.5.5 ARINC Architecture-E—Architecture-E is a combination of a physically centralized and distributed architecture. Architecture-E also is distributed logically. The system architecture is illustrated in Figure 4-10. Because the architecture is highly integrated, the core module is shared by several applications. The executive software supports multiple applications and invokes strict segregation between application software.

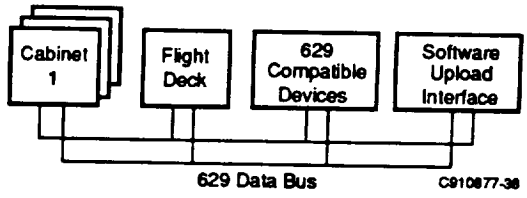


Figure 4-10. Architecture-E

Segregation between applications is achieved by robust partitioning between application memory space allocation. Communication between applications themselves and between applications and health monitoring functions is performed through executive software services. Each application will have its own memory space, which is accessible by the application and the executive through specific services only.

Fault Tolerance Considerations—To meet the safety and availability aims for critical functions, software dissimilarity is applied. For flight-critical functions, hardware dissimilarity is essential. This means that two different designs for each module shall be required.

4.3.5.6 Boeing 777 Avionics Architecture—The Boeing 777 avionics architecture is a hybrid between a federated and a fully integrated architecture. The architecture takes advantage of cabinet integration but maintains a federated architecture for flight-critical components. The basic architecture of the Boeing 777 avionics architecture is shown in Figure 4-11.

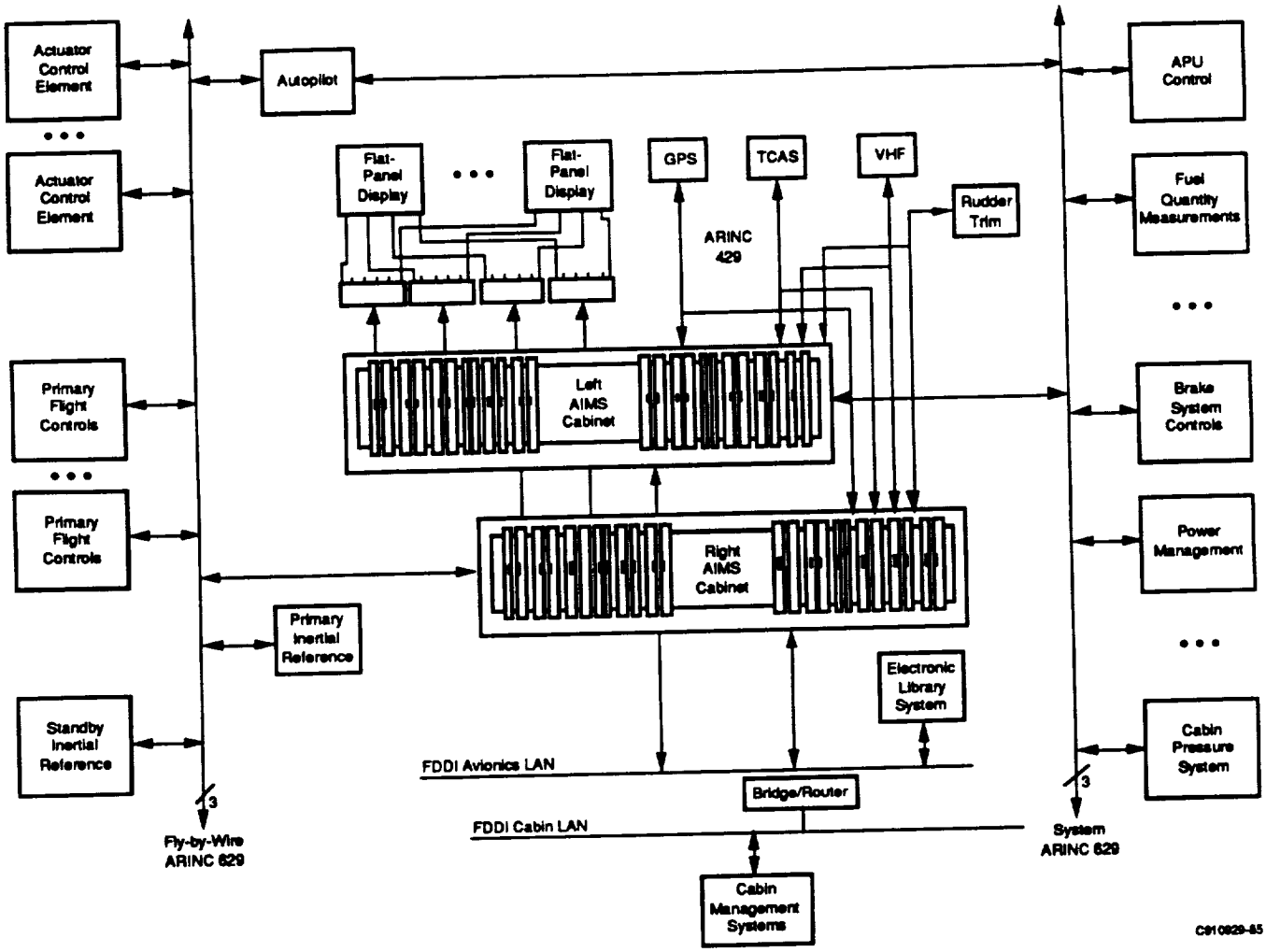


Figure 4-11. Boeing 777 Aircraft Functional Diagram

A key subsystem of the 777 avionics architecture is the AIMS. It consists of two integrated cabinets that are replicated for redundancy. Each cabinet contains four core processing modules, four standard I/O modules and two power supply modules. Two processing modules have graphics capability, one provides basic processing functions and one is dedicated to the FDDI communication interface. Each I/O module provides ARINC 629, ARINC 429, analog and discrete signal interfaces. The AIMS architecture is shown in Figure 4-12.

Seven primary applications sharing the processor and I/O resources are implemented in each cabinet. Some applications, such as displays, are replicated twice in each cabinet, providing high integrity and availability.

The information transfer system is based on a multiprotocol communications network and provides avionic integrity and availability through the use of redundant ARINC 629 data buses, ARINC 429 buses, Taxi buses, and FDDI networks to fulfill performance, fault tolerance, and cost-effectiveness requirements. Communications between cabinet modules is provided by the SAFEbus™ backplane. Primary communications between LRUs in the airplane and the AIMS system is provided by two sets of triple-redundant ARINC 629 buses: the Fly-by-Wire 629 bus set and the System 629 bus set. Only the Fly-by-Wire 629 bus set connects components that are critical to airplane flight, examples of which are:

- Primary flight control computers,
- Actuator control elements,
- Air Data Inertial Reference Unit (ADIRU),
- Secondary Attitude Air-Data Reference Unit (SAARU),
- Air data computer primary flight sensors.

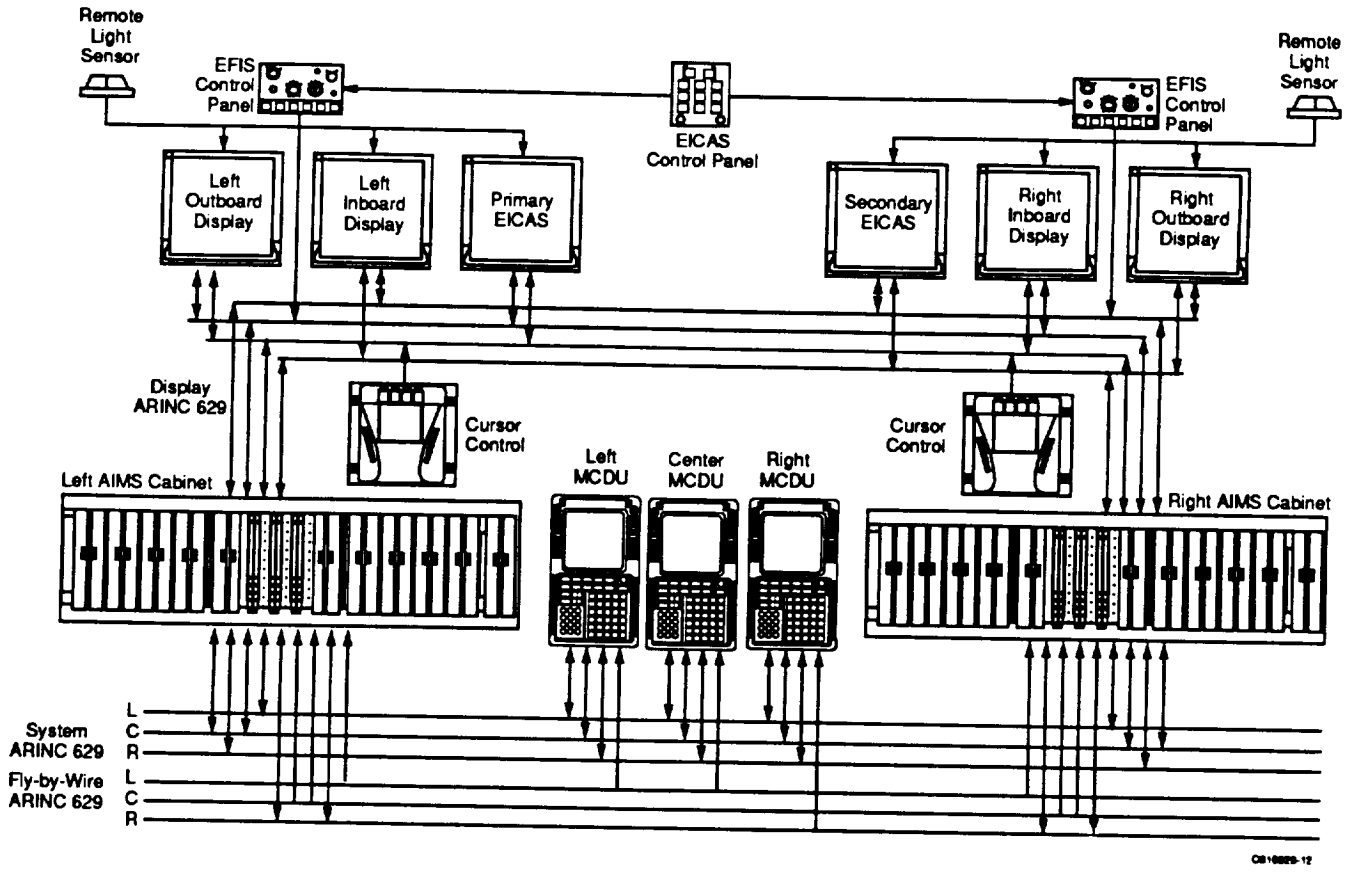


Figure 4-12. AIMS Architecture

Other less critical LRUs (radios, printers, and some control panels) also reside on the System 629 buses.

Gateway and bridge functions are incorporated within the AIMS. AIMS provides bridges between the Fly-by-Wire 629 bus sets and the System 629 bus sets, and gateways from 629 buses to other data bus interfaces.
Other data interfaces are incorporated to match subsystem interface requirements. The FDDI LAN standard provides high data throughput required by the electronic library and cabin management portions of the airplane. The FDDI network is defined by the ANSI X3T9.5 FDDI committee. The FDDI network, which is presently used in the Space Station Freedom avionic architecture, provides a fault-tolerant high-throughput (100-Mbit/s data rate), multinode (up to 500 network nodes) transmission medium that can span distances up to 2000 meters.

The ARINC 429 bus is used to maintain compatibility with some existing equipment that will not be redesigned to incorporate the newer ARINC 629 standard. Similarly, analog and discrete interfaces support signals from sources where it is not cost-effective to provide sophisticated data bus interfaces.

4.3.6 Strawman Architectural Framework

A strawman COTS+ architectural framework for Earth to Orbit (ETO) launch vehicles, Lunar and Mars Transfer vehicles (LTV/MTV), orbit, and excursion vehicle future manned missions is presented as a study point-of-departure baseline. This is shown in Figure 4-13. The framework incorporates Boeing 777 airplane avionic architecture and features; two AIMS cabinets are integral to the architecture. The framework is intended to replicate Boeing 777/AIMS architecture to the greatest extent, thereby providing this study a bottoms-up assessment of COTS utility.

The baseline framework incorporates commercial IMA system architectural concepts and follows the concepts of modular network-oriented Pave Pillar and MPRAS architectures. The architecture is flexible and accommodates most types of avionic equipment, including equipment without 629 bus interfaces and/or nonmodular LRUs. The strawman comprises a number of LRUs and cabinets that contain equipment to do the bulk of the processing and any local I/O to sensors, actuators, and indicators that do not justify the use of remote electronics.

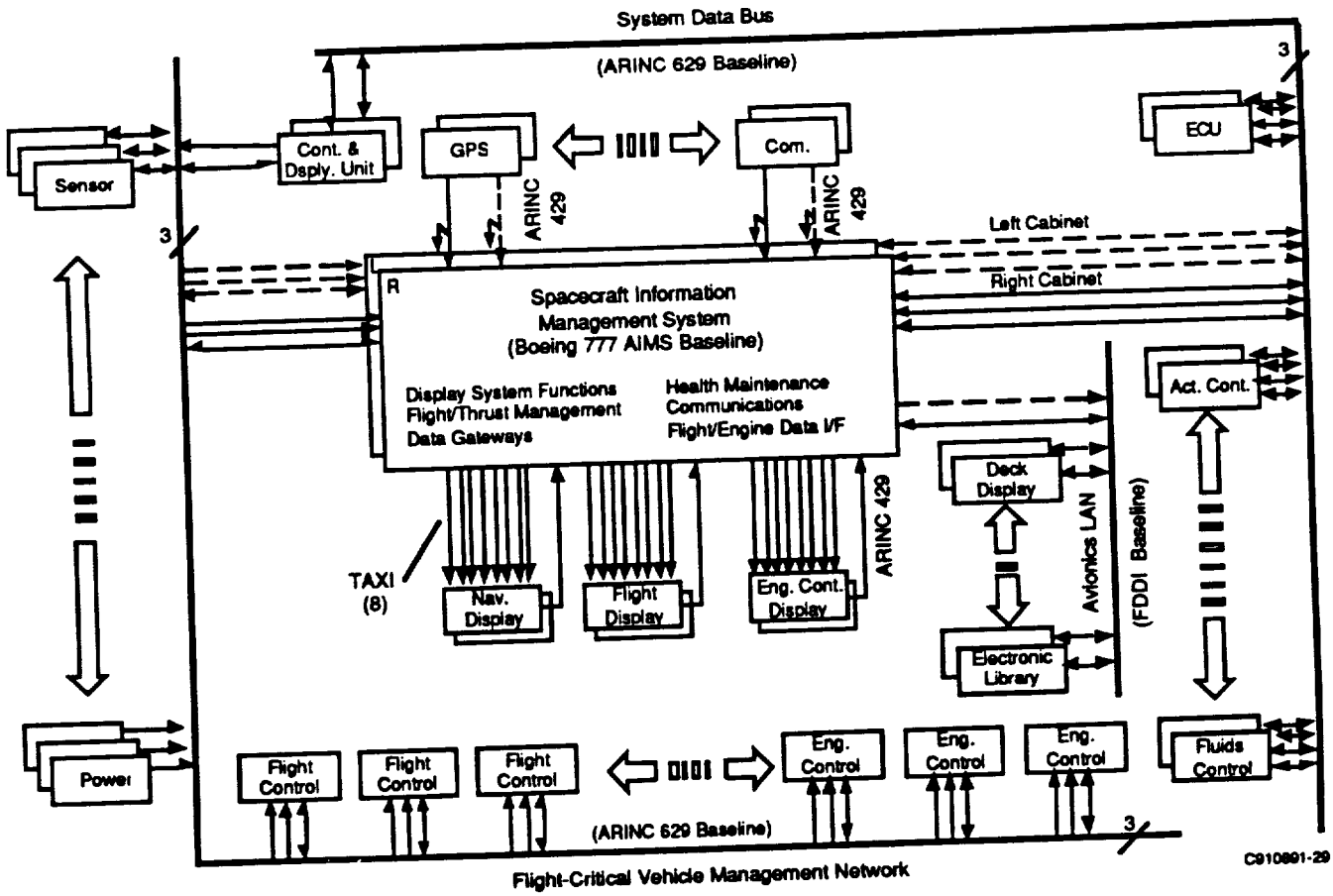


Figure 4-13. COTS+ Architecture Framework

Two ARINC 629 bus networks are incorporated within the architecture. The cabinets are connected to one another and to flight-critical components by way of a fly-by-wire ARINC 629 data bus called the Flight-Critical Vehicle Management network. A second ARINC 629 network, the System 629 bus set, called the Systems Data Bus, provides interfaces to flight-critical functions. ARINC 429 data buses provide point-to-point communications for equipment with existing 429 interfaces. An FDDI LAN network is available for high-throughput electronic library displays, cabin LAN resources, maintenance and/or training data-base mass storage, and maintenance access to the avionics. Several Taxi buses are used economically to provide high-speed 100-Mbit/s, one-way, packed data to cabin displays. The Taxi bus requires a much simpler interface and less hardware than the FDDI network, which transfers data at the same rate.

Because the strawman framework is flexible, it will be possible to modify the framework to include other networks and subsystems. Gateways can be provided to include other networks such as, the linear token-passing bus (LTPB), the high-speed ring bus (HSRB), or the MPRAS high-speed data bus (HSDB). Established subsystems connected via these networks can be integrated within the COTS+ architecture.

4.3.7 Strawman Architectural Configurations

The strawman COTS+ architectures for launch and transfer vehicles are presented to illustrate application of the point-of-departure architecture. The two architectural configurations are shown in Figures 4-14 and 4-15 for transfer and an unmanned launch vehicle, respectively. These configurations represent examples of how a strawman framework can be modified or adapted for different missions or specific applications. Similar configurations may be developed for orbiting stations, excursion vehicles, and habitation modules.

The key features allowing use of the COTS+ framework for the various applications or missions are as follows:

- Scalability upward or downward to implement (1) more or less capability and/or performance or (2) more or fewer networks and/or functions.
- Fault-tolerant designs, fault containment within defined boundaries, and the ability to maintain system integrity.
- Effective validation of designs to assure that the avionics does not compromise flight safety.

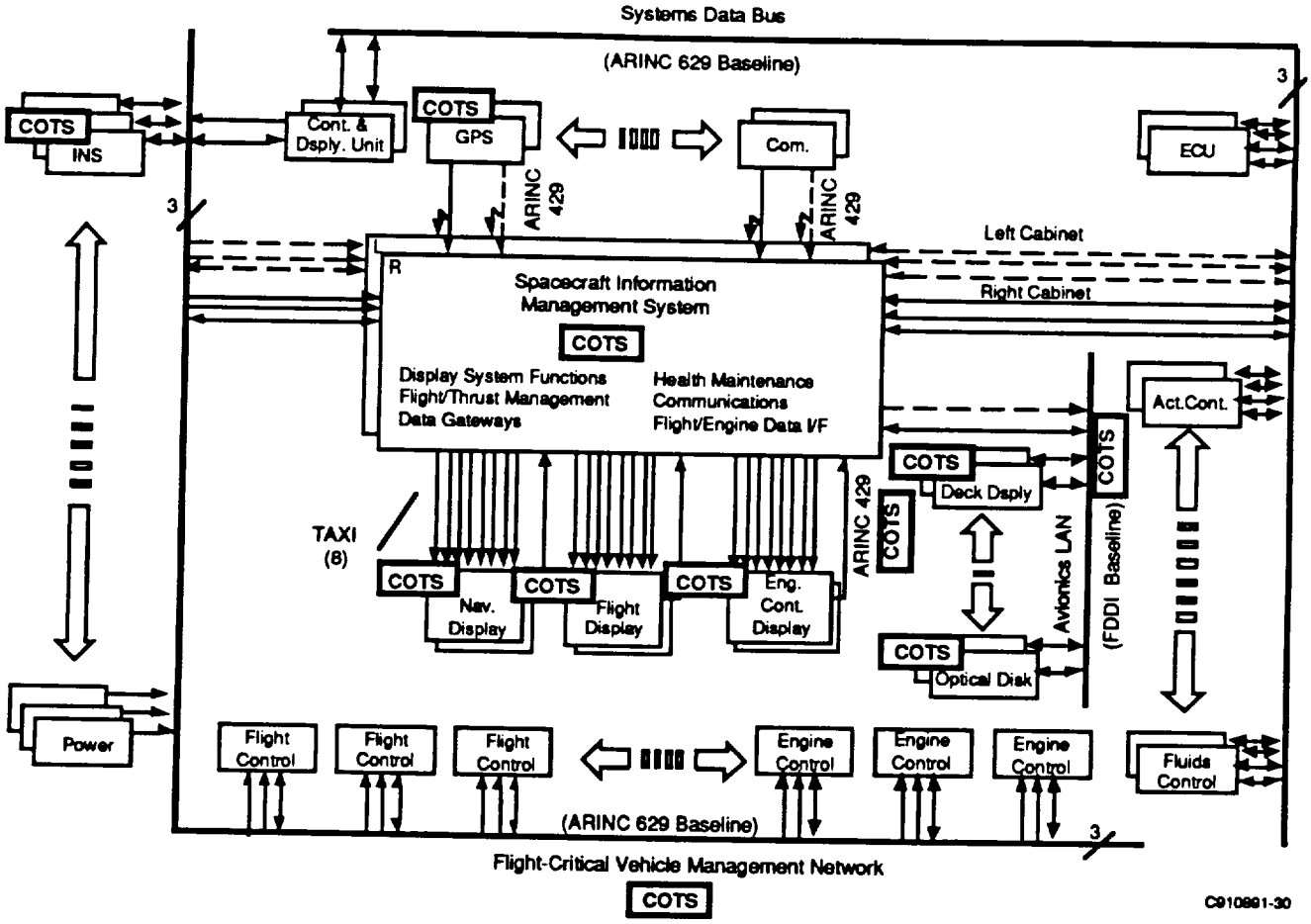


Figure 4-14. Lunar Transfer Vehicle Configuration

4.3.7.1 Transfer Vehicle Configuration—The Lunar and Mars Transfer Vehicle strawman architecture incorporates several COTS+ products described within this study. These products are identified within a double-boxed COTS label within Figure 4-14. The configuration is identical to that of the baseline framework.

4.3.7.2 Launch Vehicle Configuration—The launch vehicle strawman architecture requires more interfaces and subsystems than the baseline framework; additional interfaces to monitor and control booster avionics are required. Fewer functions are required, however, in other areas. The unmanned launch vehicles do not require functions related to manned vehicles; therefore, displays, display interfaces (FDDI) and environmental control units (ECUs) need not be provided.

A booster strawman architecture is represented in Figure 4-15. Physical partitioning of engine controllers to remote locations within the core vehicle is incorporated. Booster avionic functions are restricted to health management, control sensing and actuation, and pyrotechnics.

4.3.7.3 Orbital Vehicle Configuration—The orbital vehicle architecture generally will be more complex than that exemplified by either the launch or transfer vehicle strawman configurations. The vehicle may be partitioned into many avionic station environments, each with several major systems within the infastructure. Independent station architectures may exist, each exhibiting a COTS+ architectural framework in which monitoring, communicating, and control between stations may not exist. Interconnected stations, however, will use the fault tolerance features of the COTS+ architecture to communicate in a fail-safe manner.

4.3.8 Architectural Partitioning

The strawman architectures are physically partitioned to separate and place all COTS+ components in environments within their environmental operating ranges. This favorable juncture is realizable because of the study premise that changes to either the vehicle, architecture, and/or component requirements will be made to ensure the integration of COTS+ products within space avionics. It is also possible because the COTS+ architecture allows physically distributed components and equipment.

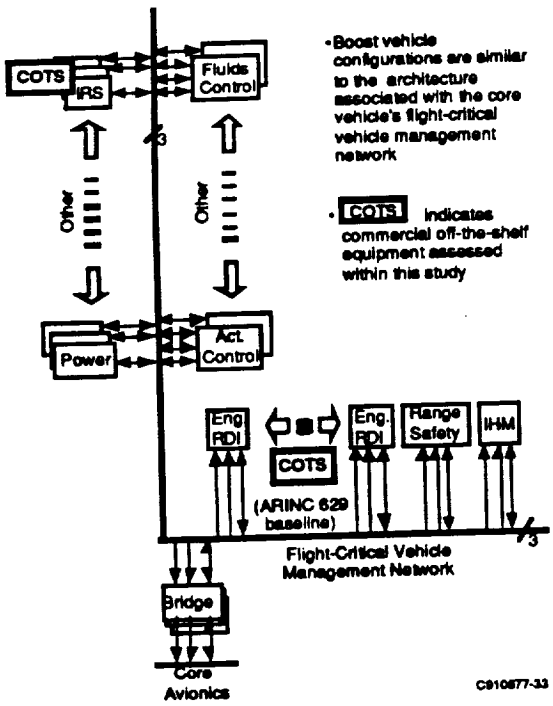


Figure 4-15. Booster Strawman Architecture

Physical partitioning of the transfer vehicle architecture is illustrated in Figure 4-16. Almost all COTS+ products are grouped and located within a common environment; this can be an easily accessible, controlled-environment equipment bay adjacent to the flight deck. The COTS+ INS, however, must be mounted at specified locations. To accommodate the INS, either the environment around it must be controlled or the product must be modified to function at its required location.

4.4 Data Networking

4.4.1 Introduction

The spacecraft data communications environment is a highly specialized communication network that manages the flow of data from multiple sources and/or sensors in real time. This data is handled at the priority needed to ensure safe, reliable spaceraft operation.

Commercial aircraft data link protocols are based on the Open System Interconnect (OSI) reference model and are used to facilitate interprocess communication among a

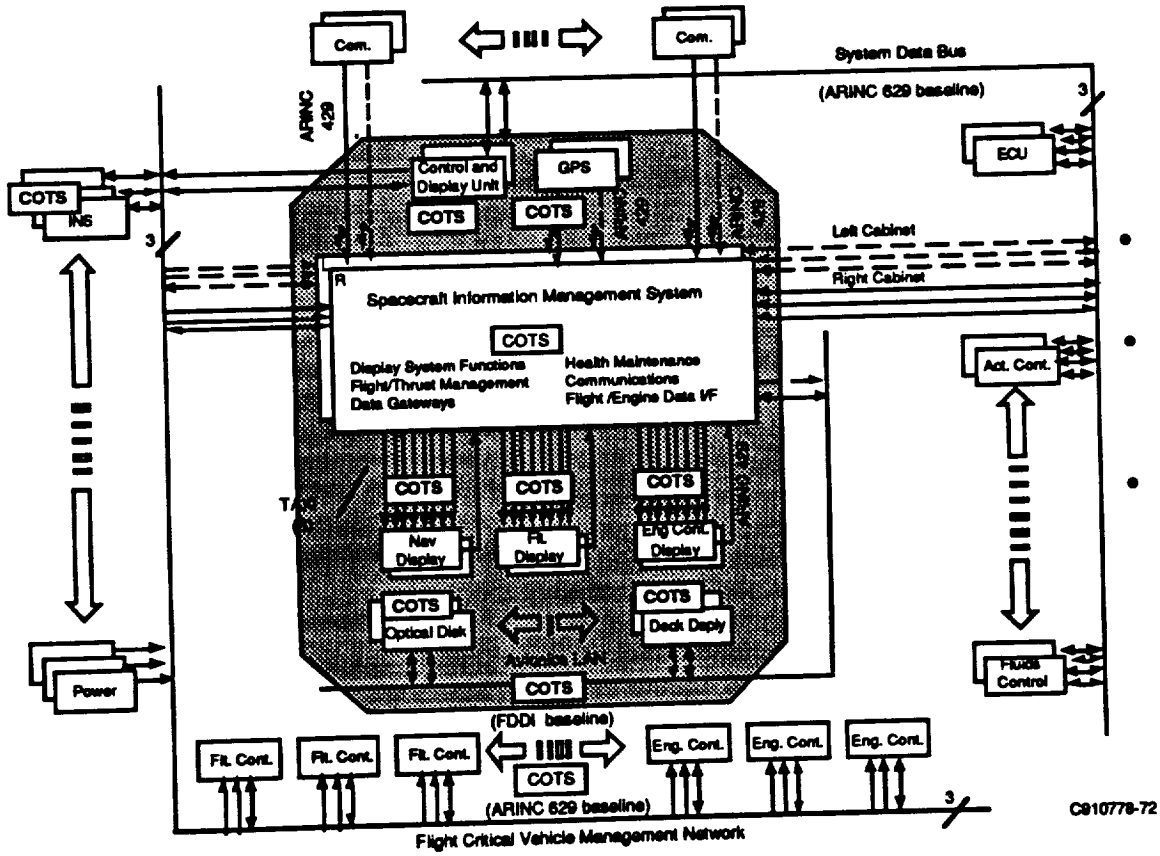


Figure 4-16. Transfer Vehicle Architectural Partitioning

variety of computing elements connected to different data buses, LANs, and other communication media. Typical data sources include, but are not limited to, Satellite (SatCom), Mode S Transponder, and Aviation VHF Packet Communication (AVPAC) equipment. These systems communicate with ground-based and space-based communication systems that are part of a global communications network. Collectively, this system of communication is referred to as the Aeronautical Telecommunications Network (ATN).

An effective data networking concept ensures interoperability of communication among user systems. Messages can originate from one end system and be directed to another end system, such as from a spacecraft central maintenance system to a central maintenance facility thousands of miles apart, while being routed via a variety of physical links, with complete transparency to the end users.

This subsection provides design guidance for the assessment, development, and use of commercial protocols required to exchange digitized data in a spacecraft OSI environment. The OSI reference model provides various functions and services for communication among different systems. COTS+ IMA-based systems provide a transparency of OSI protocols, including its functions and services to the user and application programmers.

4.4.2 Networking

The amount of communication between spacecraft avionic systems and space/ground facilities as well as between various onboard avionics systems is ever increasing. A vital design aim for COTS+ IMA-based systems is to make the interconnection mechanism transparent to the end users. To achieve user transparency, standard procedures must be followed when implementing the protocol needed for interconnecting two networks.

Internetworking in the ATN environment, where different computer networks are interconnected using OSI protocols, is ensured by compliance with ISO 8208. This ISO standard ensures interoperability of different computer networks. The application of OSI networking principles satisfies the following objectives:

- Meet the communication needs of equipment with different levels of performance;
- Allow transition of technology;
- Provide growth, capability, and interchangeability;
- Interconnect with existing networks exterior to the aircraft;
- Provide communications structures consistent with the constraints of fault tolerance and dispatchability.

4.4.3 Examples of Data Networking

The high level of integration within the COTS+ IMA system requires communication between various spacecraft systems and their subsystems. Some systems that depend on each other or are located in the same area naturally form a network group. These groups are connected to other systems in a networked group or individually, which results in a need for an interconnection mechanism between these networks. A number of interconnection methods are used, depending on the characteristics of the networks to be interconnected.

4.4.3.1 The Repeater Function—A repeater is the simplest mechanism for extending the geographical boundaries of similar computer networks. Its function is to receive a message and then retransmit it, regenerating the signal at its original strength.

4.4.3.2 The Bridge Function—A bus bridge interconnects physically distinct networks having different physical layers but a common data link and upper layers. The bridge receives all messages on each computer network of which it is a part. The destination address of the received message is checked by the bridge, and when a message intended for a station in a different network is recognized, the bridge transmits the message on that network. The bridge connection implements a store-and-forward function, since messages are temporarily stored in the bridge and then forwarded to another network. Within LANs, a bridge is also capable of resolving any frame format or other differences between the two media access control methods. Only the physical and data link layers are needed to connect similar buses.

4.4.3.3 The Router Function—The router interconnects computer networks that have different physical and data link layers but have a common protocol for the network and upper layers. The function of the router is to direct the message through intermediate nodes. Two addresses must accompany messages sent through intermediate nodes. The first is the address of the final destination node, which remains constant as the message traverses the network, and the second is the address of the next node along the route. The second address changes as the message moves from node to node along the route it takes through the network.

4.4.3.4 The Gateway Function—The gateway function resides at the highest level of internetworking. The gateway provides the flexibility needed to interconnect computer networks with completely different architectures and different protocols. Typical functions of the gateway include:

- Message format protocol,
- Address translation,
- Protocol conversion.

All layers of the OSI protocol are required to provide interconnection for the applications.

4.5 Fault Tolerance

4.5.1 Introduction

The COTS+ architecture should be implemented to take full advantage of fault-tolerant design. Fault tolerance is the ability of equipment to provide its function and to continue operation in a defined manner after one or more faults have occurred. A fault may be the failure of a hardware component or a defect in the implementation of the design in hardware or software. Continued operation spans the range of performance from full operation of all functions to various defined levels of degraded operation.

Fault-tolerant concepts have been developed to meet the need for high reliability, and airlines have recognized its potential for enabling avionics maintenance to be performed on a scheduled basis. If a module, or a function in a module, fails in a fault-tolerant system, the system can automatically reconfigure to accommodate the failure and then continue satisfactory operation until a scheduled maintenance opportunity, at which time the faulty module can be repaired or replaced.

Three processes need to take place for fault tolerance to be achieved: first, he fault needs to be detected; second, the faulty component need to be identified and isolated; and third, system resources must be reconfigured to eliminate adverse operational fault effects.

The desire for a function to be fault tolerant significantly affects equipment design. To continue operating, either resource redundancy or a hierarchy of tasks must be sacrificed. Monitors and switching mechanisms are also required to recognize faults and provide a reconfiguration path.

4.5.2 Application

Two distinct goals may be achieved by designing a fault-tolerant function; both goals are COTS+ objectives. One goal relates to the dependability issue of how to provide operational integrity such that flight-critical functions will be performed safely. The other is to provide sufficient equipment availability to receive an economic benefit from deferred maintenance. These goals are quite diverse in their objective and will influence how the fault-tolerant design should be implemented. The influence of these two goals on design are discussed in Subsections 4.5.2.1 and 4.5.2.2.

The specification of requirements for an avionics function establishes, when necessary, the desire for fault tolerance and the extent to which it should be achieved. Generally, it is necessary to specify allowable modes of degraded operation, that which constitutes failure of the function, and the time interval within which faults are expected to be absorbed without reaching functional failure.

4.5.2.1 Functional Integrity—When a function is required to possess high integrity in its operational performance, several factors, discussed below, are important.

A single fault must not be allowed to cause a functional failure that creates a potential hazard. This applies to hardware failures throughout the system, from its sensors and data sources, through its computations, to its actuators and annunciations. This also applies to the potential for defects in the design of software-implemented functions.

The monitoring must provide sufficient coverage of the equipment circuitry to ensure that no failure that might lead to a hazard can escape detection. The ability of the monitors to perform their intended function and cause reconfiguration of the system cannot be compromised by the fault itself.

Sequences involving multiple faults are considered analytically to establish that the potential for an undetected hazardous situation is sufficiently remote. This combines considerations of failure rate, detection coverage, and exposure time. (Exposure time is the interval of operation since the function was last confirmed to be free of faults.)

The industry-accepted standard for the integrity of a system performing flight-critical functions is that the probability of a hazard resulting from total functional failure be extremely remote. Achieving these low probabilities depends on low failure rates, high monitor coverage, and short exposure times.

Once the responsibility for continued safe operation has been vested in a system, there shall be assurance that the integrity required is in fact achieved. This is accomplished through verification testing to show that the implementation meets the specification over the range of anticipated operational conditions and environments.

4.5.2.2 Functional Availability—If the purpose of designing a fault-tolerant function is economic advantage, a different set of factors influence the design.

High-availability equipment is designed to sustain multiple faults and continue to operate. It does not necessarily need to be completely free from defects. In this type of equipment, a single fault disabling a function or some undetected faults can be tolerated, providing they do not occur often.

The implementation will be judged primarily on the economic tradeoff between acquisition cost and crew workloads. The desired duration of continued service and acceptable levels of degraded performance must be specified, just as for the high-integrity case.

4.5.3 Design Considerations

Fault tolerance can be achieved by a wide array of hardware and/or software design techniques. For hardware, the basic approach is to check the correctness of input and output signals and multiple processors of the same or different types. For software, a similar approach uses multiple, possibly different, versions of code to perform the same function and, again, the outputs are compared or voted.

The design of a fault-tolerant function is guided by a set of specifications stating integrity and availability goals. These requirements are just as relevant as the operational performance of the equipment.

The specification of fault tolerance is conveyed by several distinct parameters. Several are listed below; others may exist, depending on the nature of the function being defined. These parameters must be defined for COTS+ future manned missions. The following functions are required:

- The desired acceptable operation after a fault for each mode of normal operation.
- Functional failure stated in terms of lack of capability below some minimal level.
- The tolerable risk of functional failure resulting from a single fault.
- The system reaction time to detect a fault and accomplish reconfiguration.
- The tolerable risk of functional failure resulting from a combination or sequence of faults.
- The mission time over which the function is expected to absorb faults and continue to provide its intended operation.

4.5.3.1 High-Integrity Data—As equipment resources expire, the integrity margin of continued operations diminishes. These factors are constraints on the design of the resources performing the primary functions of the equipment.

Some form of functional redundancy must be chosen to provide the ability to continue operation in the presence of a fault. This is necessary if there is a requirement to survive any single fault and if most or all of the functional capability must be maintained. The COTS+ quad channel and AIMS architecture provides this redundancy.

Isolation of resources is also necessary. The various redundant components must operate independently of one another. The monitor of a function must also operate independently of the function itself. This independence shall be such that no normal, abnormal, or failure event can create a common effect in the redundant resources or in a function and its monitor. The Boeing 777 AIMS architecture and the MPRAS cross-channel comparators/voters provide the needed isolation.

The monitoring must be highly effective. It needs to provide coverage of all the operational components and be capable of detecting all hazardous failures. It must periodically be exercised to ensure that it is capable of both detecting anomalous behavior and communicating to the reconfiguration mechanism.

The implementation of a high-integrity function must meet its operational performance requirements and its fault-tolerant design specifications with the assurance that design defects are acceptably remote. This implies that the design needs to fulfill its intended function and be free of any unintended function. Such validation is accomplished through a combination of testing and analysis of the equipment to establish proof of correctness.

When equipment resources expire, the crew is informed that even though the function is performing all intended operations, the risk of functional failure has increased, and the crew may need to operate with limitations or initiate maintenance action.

There is a question of how much information, if any, is needed to inform the crew that the fault-tolerant system has automatically reconfigured to accommodate faults. The concern is that the crew should be aware when the system is one or two failures away from reversion to emergency procedures so they can be prepared to assume control or institute failsafe procedures. On the other hand, continuously lit caution lights or continuously displayed caution flags or messages soon lose their effectiveness.

When equipment remains in service and accumulates faults, it will gradually degrade. At some point, the spacecraft cannot be launched, if on the launching pad, or con-

tinue assured operation, and maintenance becomes necessary. Preferably maintenance will be performed at a convenient time prior to ultimate functional failure. For maintenance to be effective, the accumulated, but masked to normal operation, failures must be visible to the maintenance crew. This implies that fault history is maintained and that interrogation capability is included in the implementation. Once history is provided, there will be a means of updating the history when the equipment is partially or fully restored.

Many systems contain functions with varying integrity requirements. Whenever functions of differing integrity are combined in a system, the equipment needs to be treated according to the highest level of integrity. An exception to this can be achieved through partitioning of the resources and functions according to levels of integrity. If functional partitioning is employed, it must be managed by resources of the highest integrity in the system.

4.5.3.2 High Availability Design—Similar to the high-integrity function, the implementation of equipment specified to achieve high operational availability has unique factors. These factors are constraints on the design of the resources performing the primary operational functions.

Equipment redundancy is applied to increase availability. In the COTS+ architecture it is essential; however, if the function is not involved in any flight-critical application, task shedding may also be useful. With task shedding, as resources expire due to failures, the services performed by the equipment are reduced in a specified manner to concentrate the remaining resources on the most desirable operations.

If total functional failure is not hazardous, the extra effort required to ensure isolation of redundant resources is not necessary; however, it is good design practice to isolate a monitor from the function being monitored.

Monitor effectiveness is robust to significantly improve availability. However, minor lapses of coverage and undetected failure to an insensitive state may not detract from the availability achieved.

Since improved functional availability is the main goal, maximizing the MTBF of the equipment is one implementation strategy. This implies the need to keep complexity to a minimum while creating as many success paths as possible, which in turn allows a tradeoff to be made between failure rate and level of redundancy. For very reliable devices, a single implementation may be chosen, applying redundancy only to selected components that do not have inherently high reliability. The COTS+ architecture minimizes complexity with its quad channel implementation and applies redundancy to its modular components.

4.5.4 Implementation Technique

COTS+ equipment is composed of both hardware and software resources. The fault-tolerant enhancements, like the operational characteristics of the function, are distributed between these resources. Hardware and software are used to complement one another in performing fault detection, identification and reconfiguration.

4.5.4.1 Hardware Implementation Techniques—Hardware fault tolerance is achieved by a variety of means. The specific avionics application influences the methods used. The following paragraphs describe typical COTS+ hardware techniques that contribute to a fault-tolerant configuration. Technique topics discussed are:

- Input and output checking
- Computational performance monitoring
- Partitioning
- Mid-value select
- Plurality voting
- Redundancy
- Dissimilar hardware
- Monitoring
- Reconfiguration
- Fault tolerance renewal

Input Checking—Reasonableness checks are used for single-input sources to determine if their signal falls within prescribed limits before it is passed to the computation process. Comparison is used when two inputs are available. The two inputs are compared, and if different by more than some preset value, the inputs are rejected and the computation uses previously obtained inputs. For three or more inputs, the inputs are voted and the majority or middle value is used.

If invalid inputs continue, the input source is considered to have failed and alternative input sources are invoked.

Computational Performance Monitoring—Computational performance is monitored through watchdog timers and self-checking pairs (SCPs). Watchdog timers monitor the execution time. If the time exceeds a prescribed limit, the processor is taken off line for diagnostic testing. If the processor passes the diagnostic testing, it is reconnected to the system. SCPs provide bit-for-bit comparison of two paired signals. If the SCP signals or data do not match, both sources are considered faulty.

Alternatively, different versions of software, usually with reduced execution time and computational capability, could be used.

Output Checking—Output checking is also used in fault-tolerant systems. Like single inputs, output from a single processor is subjected to reasonableness checks. For a pair of processors, the outputs are compared in a manner similar to that for input comparison. If the outputs do not match, both processors are disconnected and diagnostically tested to identify the faulty processor, if any, before being reconnected to the system. For several processors, the outputs are voted and the majority value is passed on through the system. The processor(s) producing the rejected output(s) are taken off line for diagnostic checking.

Partitioning—Partitioning, the physical and systematic separation of functions, is used to limit fault propagation throughout the system and therefore reduce the probability of system failure. Partitioning also minimizes system test effort and the time needed to perform hardware and/or software modifications.

Mid-value Select—Mid-value select is a simple algorithm for enabling a system to tolerate a single fault in any information source whenever the system has three or more sources of the same information. The basic technique is to ignore the maximum and minimum values of any input parameter. The remaining values is within an acceptable tolerance, assuming no more than one failure. This approach also provides some probability of tolerating two failures, especially if it is combined with reasonableness tests or if there are more than three sources of information.

If two or more redundant input sources have passed reasonableness checks, the average (mid-value) signal is used if no other condition dominates the selection of either the highest or lowest value.

Plurality Voting—Plurality voting is a technique for enabling a system with at least triple redundancy to tolerate single output faults. If all redundant outputs are summed, and if all outputs have limited authority, a system can be designed so that the sum will always have the correct value, no matter what the value any one failed output takes. Like the mid-value select technique, plurality voting can also tolerate certain classes of double faults.

Redundancy—Hardware redundancy is essential since hardware elements expire due to failures over time—especially over the duration of extended or deep-space missions. Unfortunately, as hardware is added to create redundancy, the overall system failure rate also increases. For high-integrity functions, this is a necessary cost of providing the service.

Assuming that the same level of technology is employed, a fault-tolerant implementation has a lower mean time to first failure than a non-fault-tolerant design due to the added number of parts. Whether this complication can be offset in terms of cost and utility is usually determined by the system designer. The COTS+ maintenance concept circumvents this complication.

Well-established mathematical models and formulas predict the improvement in availability using multiple components with a given reliability. They show a definite limit on the benefit to be gained by adding redundant elements. The COTS+ philosophy will be to circumvent this limit by providing cold spare COTS+ components to replace failed redundant elements. Further discussion of this concept is provided in Subsection 3.4, Testability and Maintainability.

Wherever redundant circuits are used or data from redundant sources is processed, isolation must provided. The benefit of the multiple resources may not be realized if a single event or failure has the same effect on several or all of the circuits. This can allow the equipment to misbehave if the monitoring is unable to detect such events.

Analytical redundancy is sometime used to replace failed sensors in fault-tolerant systems. In the case of a sensor failure, algorithms can use data from remaining sensors to compute a probable signal from the failed sensor. The computed signal is then treated as a valid input by the rest of the system. Similarly, in the case of a flight control actuator failure, the remaining actuators and control laws can be automatically reconfigured to compensate for the failure.

Dissimilar Hardware—For functions that must operate with high integrity, implementation using dissimilar hardware is considered a means of protection from certain types of design defects. Such configurations have unique benefits as well as liabilities.

Dissimilar implementation may be the only method of avoiding common mode faults in redundant circuits that result from or are aggravated by design defects. Faults may be more easily detected by simple monitors, and the potential hazard of latent faults is reduced.

The level of effort necessary to create a dissimilar implementation has several added liabilities. The most obvious is the multiplication of development costs and efforts for the design of multiple circuits and their associated verification. Each different version must be demonstrated to have complete operational capability. More subtle is the need to verify the dissimilarity itself. If the function is to derive protection from the presence of dissimilarity, that dissimilarity needs to be proven and shown to be without any opportunity for common mode faults.

Monitoring—Generally, monitors fall into three categories: paired comparison, which is the comparison of

pairs of processes; absolute comparison, or the comparison of a parameter relative to a fixed threshold; and detection of an event. Each monitor must be implemented with a level of integrity consistent with the function being observed. This can mean either that the monitor be fail-safe or replicated to ensure that detection occurs.

Monitors implemented in hardware typically are dedicated to the specific circuit being observed. However, hardware-implemented monitors can also observe the performance of software-implemented functions. In addition to detecting an event or an exceeded level, the monitor should also communicate the abnormal state. This may be done via an interrupt to a processing resource, a flag that is passively interrogated by another process, a trigger for reconfiguration, or an annunciation for the crew to resolve.

Reconfiguration—Reconfiguration is the process or act of changing the active resources within the equipment. Examples of hardware reconfiguration devices are voters, reset pulses, interrupts, and data steering switches. When implemented in hardware, these reconfiguration devices generally are dedicated to specific single parameters or data paths. This is a necessary compromise due to the complexity of these types of circuits.

Once reconfiguration has taken place, the equipment operates at a lower level of dependability. A failure has been absorbed by the system, and it may not have the ability to sustain another similar fault. Careful consideration must be given to returning to the original system state. A balance between recovering from transient faults and retaining protection from new possible failures within the reconfigured state must be implemented.

Fault Tolerance Renewal—Fault tolerance renewal is an event that establishes that a component is fault free to some confidence level. The mathematics of predicting failure probabilities provide estimates from the last point of fault tolerance renewal.

If no method is available to ensure that a component is fault free, the exposure time grows to infinity and the probability of a failure approaches unity. Fault tolerance renewal processes may be included in the equipment to detect otherwise latent faults, thereby limiting exposure times and reducing hazard probabilities.

Fault tolerance renewal can be accomplished by scheduled self-test, periodic maintenance inspection or test, on-condition maintenance test, or original manufacturing test. Each of these techniques provides a limit on the exposure time. All the hardware elements of the equipment need their exposure time established to compute hazard probabilities. The COTS+ uses CMC and integrated health maintenance to minimize exposure time and ensure, with a high probability, that a component is fault free.

4.5.4.2 Software Implementation Techniques—Software does not wear out and, therefore, does not have a failure rate as a function of operating time. The concern with software is the possibility of design defects. More sophisticated systems tend to vest their complexity in the software implementation. This, in turn, increases the potential for residual design defects, even after extensive verification and validation testing. The application of fault tolerance to software implementation attempts to neutralize the effects of any residual design defects.

The paragraphs below describe typical COTS+ software techniques that can contribute to a fault-tolerant configuration. The topics of N-version programming, recovery blocks, consensus, exception handlers, monitoring, reconfiguration, and fault tolerance renewal are discussed.

N-Version Programming—N-version programming is a widely used fault-tolerant software technique. In this approach to fault tolerance, two or more versions of software are developed independently to accomplish the same task and to a common specification. These versions can be sequentially run on the same processor; however, generally they are run in parallel on separate processors and, frequently, as an added fault tolerance measure, on different types of processors. The outputs are then voted and the most probable value is passed to the system.

To be effective, each different software version must be completely verified. Otherwise, the residual errors may not be small, and the function may suffer frequent reductions in integrity and availability as the errors are detected. Due to the cost, N-version programming should only be considered for functions with the highest integrity requirements.

If N-version programming or any form of dissimilar redundancy is used as a means of protecting a function from design defects, the achievement of dissimilarity needs to be confirmed. Studies have indicated that similar errors can occur in different program versions, presumably due to specification ambiguities or complexities.

Recovery Blocks—The simplest form of fault-tolerant software is recovery blocks. In this approach to fault tolerance, the output of the code is subjected to an acceptance check. If it fails, the same code can be re-executed; alternatively, different versions of code can be executed until an acceptable output is obtained. If no acceptable output is obtained, the software is assumed to have failed.

The concerns with recovery blocks are the additional execution/re-execution time, the integrity of the acceptance

test, and the storage of the input for repeated computations until recovery is successful.

Consensus—A third fault-tolerant software technique is consensus, which blends features of both N-version programming and recovery blocks. The output of N-versions are compared, and if two or more agree, the output is passed to the system. If no two versions agree, the outputs of each version, beginning with the most capable, are successively tested until an acceptable output is found. If no acceptable output is found, the software is declared failed.

Although N-version software is widely used in flight-critical systems, it may not always be the proper approach. An alternative view is that if the resources needed to develop N-versions of code were applied to the careful design and complete validation of a single version, the single version would be preferred.

Exception Handlers—Fault-tolerant software also includes exception handlers for invalid operations, such as dividing by zero or computing the tangent of 90 degrees.

Monitoring—Many of the monitor functions found in hardware are also appropriate for software implementation. In addition, software programming allows complex boundary value and parameter reasonableness checking.

Software monitors confirm that the program is executing properly by performing sequence and timing checks. In addition, an independent means of assuring valid central processing unit (CPU) operation is necessary for high-integrity applications. This is provided by using a combination of hardware- and software-implemented functions.

Software monitors are also used to confirm proper operation of the hardware functions. Such techniques as wrapping outputs back to the input plane, tracer signals on data paths, and periodic diagnostic routines are capable of achieving high levels of monitor coverage.

Reconfiguration—As with monitoring, software programming allows more sophisticated reconfiguration functions than are possible with hardware. Signal select algorithms can be applied to a large number of parameters using mid-value or weighted vote for acceptance. Equalization between sources can provide compliance for time skew or system tolerances. In addition to signal steering, processes can be activated or suspended. Exception handlers can be created to provide unique programming or execute in response to specific events. Data may be reinitialized for a repeat attempt at execution.

Fault Tolerance Renewal—Since software does not wear out, fault tolerance renewal is not necessary. Software is assumed to continue to provide its intended function indefinitely.

There is a tendency for software to degrade during the course of modifications and corrections. This is characterized by errors appearing after modification in areas of the program that were not intended to be changed.

Therefore, it is essential that proper attention be given to the verification of each extrapolated version of an existing software program.

4.5.5 Role of Monitors/Displays

Typical fault-tolerant systems require that a very high percentage of possible faults be detected and identified. Meeting these goals calls for careful design of the built-in test equipment (BITE), the tests it executes, and the reporting mechanism. BITE design should be based on the results of a fault tree analysis and/or a failure modes and effects analysis (FMEA).

4.6 Software Architecture

4.6.1 General

The functionality of the COTS+ avionics system is provided by a Common Application Software Environment that offers greater flexibility for functional enhancement. Application software development costs are likely to dominate the cost of ownership for COTS+, and it is therefore necessary to make use of modern methods of design, implementation, and test to manage those costs.

Existing avionics software is traditionally packaged with the hardware as a complete, operating avionic system. This association is being changed in future subsystems. COTS+ software may conceivably be produced by a party other than the hardware supplier; therefore, the method of procuring avionic software is likely to change. This will result in new business opportunities for traditional avionics manufacturers, software developers, and others who have yet to do business with primes. It is expected to be advantageous to users and suppliers and eventually to reduce avionic system cost.

Because application software development costs are likely to dominate the cost of ownership for COTS+, minimizing this cost is the main driver for the standardization described herein. However, there are additional standardization benefits, such as the reuse of reliable verified software developed in other COTS+ applications.

Software applications are only one of many functional elements of the COTS+ architecture that offers a building-block approach. For the software building-block approach to be successful, a common application software environment is necessary that is consistent with both system and hardware architecture.

4.6.2 The Software Architecture

The COTS+ AIMS/IMA software architecture performs a key role in achieving COTS+ goals. Components of the software architecture are:

- Application software that performs the avionic functions.
- Core software that provides a standard and common environment in which application software executes. The core software is further partitioned into:
  - A COTS+ operating system (OS) that manages logical responses to applications demands. OS functions include allocating processing time, coordinating communications channels, and managing memory resources. The OS function maps application requests to system-level logical mechanisms and provides uniform logical interfaces to the applications. The system health monitoring function within the OS initiates error recovery or reconfiguration strategies that perform a specific recovery action.
  - A hardware interface system (HIS) that manages physical hardware resources on behalf of the operating system. The HIS maps logical requests made by the resources and assures fault containment within the physical boundaries of the hardware.

    The software forming the HIS maps the particular implementation of hardware onto the operating system. This software is unique to the hardware implementation. Also at this level are BITE and BIT functions that are also unique to a particular hardware implementation, as are any hardware-level fault-containment mechanisms.

    Hardware provides the physical means of access to the COTS+ system via the backplane bus, together with the memory management and other partitioning functions, which ensure that applications cannot interfere with either each other or the operating system.

COTS+ software will be loadable onboard space vehicles. This feature will be transparent to the application software. This function will be implemented using small blocks of code with well-defined interfaces. Proper attention is paid to software reliability, maintainability, modifiability, and certifiability for the code design.

4.6.3 Benefits

The benefits of providing a common application software environment include the following:

- Multiple independently produced applications may run together on the same hardware.
- The standard interface decouples hardware changes from software changes.
- Possible verification cost reduction by segregation of verification into independent processes associated with:
  - Hardware,
  - Applications software,
  - The interfacing software or operating system.
- Software portability is improved.
- Development test equipment may be standardized.
- The cost of ownership of software is reduced.

4.6.4 Language

COTS+ software is written in Ada. AEEC has adopted Ada as the standard high-order language (HOL). The features of Ada recommended for use in real-time avionics applications are documented in ARINC Report 613, "Guidance for Using the Ada Programming Language in Avionic Systems." Ada and modern design techniqueswill be applied to create software in modular form that allows applications to be partitioned to minimize the impact of software changes.

The COTS+ operating system presents the compiler with a uniform interface to hardware resources in logical rather than hardware form. The generation of Ada run-time systems is therefore greatly simplified. Although the operating system offers clear benefits to the Ada compiler interface, the interface need not be constrained to Ada, and as future languages emerge, they may be used just as effectively.

4.6.5 Software Functions

The software functions applicable to a COTS+ core processor are:

- Application software,
- Operating system software.

All data flow between the core hardware and applications is controlled via the operating system through standardized interfaces. The goal is to decouple the applications from the hardware.

4.6.6 Interfaces

Software interfaces are standardized in the form of ARINC specifications. The interfaces are:

- APEX—the applications/executive interface.
- COEX—the core hardware and HIS/executive interface.

The APEX interface completely defines the common environment for the applications. To achieve a common environment, the APEX interface requires rigorous definition.

Application programs communicate with the executive via this standard interface. APEX consists primarily of system procedure calls. This executive interface specification will be adhered to for all application software that uses the APEX interface.

The COEX interface defines the higher level functions making up the operating system and the lower level hardware-specific functions. A health monitoring recovery strategy table is defined within the operating system.

The primary aim is to provide a common environment for application software through the standard interface, APEX. A secondary aim is to provide another interface, COEX, between the operating system and the low-level primitives that map the functions onto the physical hardware. Such a feature allows the applications to be integrated with the operating system on general-purpose computers, where the interface COEX would be tailored to that environment and would provide a suitable medium for simulation. Given a rigorous definition of APEX, it will also be possible to integrate and test applications on a general-purpose computer that simulates the APEX interface. It will be possible to host a variety of applications without modifying the operating system.

4.6.7 Applications Software

The applications software is software that performs a specific avionics function.

4.6.7.1 Software Integrity—In COTS$^+$, the method and level of redundancy, fault detection, fault isolation, and reconfiguration (FDIR) is transparent to the application software. Application FDIR software is only responsible for the redundancy management of a specific function and for signal selection and failure monitoring of inputs from external sensors or other systems.

Modular software design enables the implementation of software partitions to isolate avionics functions within a common hardware environment. Application software will be independent of hardware. Some software modules may be developed by independent sources and integrated into the cabinet. Therefore, it is necessary for software within a partition to be completely isolated from other partitions so that one partition cannot cause a fault in another partition.

The application software is specified, developed, and verified to the level of criticality appropriate to its system function. Regardless of the level of criticality, applications must be partitioned from each other.

To ensure partition integrity, partition load images will be statically and separately built. They will stand alone as independent program modules, with no interdependencies with other program modules. The partition code can be used to change process scheduling attributes and thus alter the execution or state of a process within that partition. In this way the integrity of one application is not compromised by the behavior of another application, whether the other application is deemed more or less critical.

All communications between applications will be performed through the operating system, whose mechanisms ensure that there is no violation of that interface and that no application either monopolizes a resource or leaves another permanently suspended awaiting an interapplication request.

4.6.7.2 Input and/or Output (I/O) Control—In traditional applications development, I/O handling is one significant area that is very specific to the spacecraft configuration of sensors. In the interest of portability and reuse, the partitioning of the applications software architecture will identify the spacecraft-specific I/O software and partition it from the functional and algorithmic elements of the application. Such sensor I/O conditioning is logically placed as a separate function associated with the sensor. Furthermore, the COTS$^+$ approach encourages the integration of intelligence within sensors and actuators. In such cases, the sensor I/O conditioning is physically placed with the sensor. The network architecture of COTS$^+$ also allows this conditioning function to be physically decoupled from the sensor, and it may be physically placed in either the sensor or actuator itself, within a remote data concentrator, or within the cabinet. This method also provides more cost-effective management of sensor data since the data emanating from any sensor manager performing I/O condi-

tioning is available to more than one application. Replication of this sensor data function in each application is avoided, with savings in critical processing loads. This method also allows for sensor fusion, sensor data extrapolation from alternative source types in the event of failure, and, most importantly, local fault-containment strategies. The characteristics of sensor managers are determined by application needs and hardware capability. It is necessary to specify parameters that define the update rate, fusion, and conversion from raw data to engineering data and error handling.

The use of ARINC 629-compatible sensors or logical I/O conditioning has an important effect on the form of the data appearing on the network and the interfaces to functions that employ them. The use of ARINC 629-compatible sensors allows data to be made available on the network in logical form rather than raw signal form. In addition, the interfaces to functions are defined as logical data interfaces, and this has far-reaching implications in terms of ARINC characteristics. In a networked environment with logical data on the network, an approach other than a black box approach at a physical level is needed to define functional characteristics. In the COTS+ concept, software interfaces replace physical interfaces.

The provision of a generalized mechanism allows further decoupling of application software from spacecraft configuration specifics and hardware implementation. Most applications require functional data at specific rates. The design feature of applications that ties them specifically to a particular spacecraft system is the sensor handling. The removal of this function from the application increases portability, and, furthermore, it concentrates the sensor handling in a single area, allowing sensor data with specific characteristics to be available to more than one application.

The impact of change in sensor characteristics is confined to sensor data managers, thereby increasing portability and reuse of application software.

4.6.7.3 Management—The application software is invoked by the scheduling component of the operating system in a deterministic manner. The frequency and priority of scheduling required for cyclic applications will be defined to the operating system via a data block within the process list data structure.

Applications will invoke APEX interface procedures for purposes including, but not limited to:

- Initial resource allocation requests (e.g., memory allocation);
- Communication requests.

An application may or may not wish to monitor resource response at each communication. For those communications it wishes to monitor directly, the application may specify a status area corresponding to the resource channel, thus allowing the operating system to respond to events.

In providing these facilities, the operating system manages resource allocation and arbitration in this multiprogramming environment.

Software interrupts or events relevant to the applications are passed on to the application by the operating system. Other interrupts are handled by the operating system alone. These software interrupts are not vectored directly to the application but cause a specified interrupt process embedded within the application to be scheduled. Alternatively, a flag is set in the interrupt process message area that may be monitored by the application.

Applications are constrained to the resources (memory, data channel, etc.) allocated by the operating system. Potential violation of these resources, detected by the hardware, can cause immediate suspension of that application.

4.6.8 Operating System Software

The operating system software serves several major purposes in the COTS+ concept. Therefore, a standard operating system should be defined for COTS+.

The main role of the operating system is maintaining functional integrity in scheduling and dispatching application programs. It will be possible to prove a level of temporal determinism in the scheduling of all applications and to prove that this is unaffected by the later addition of lower priority applications to the system. Functions of the operating system include ensuring partition isolation, allocating processing time to the partitions, dispatching processes for execution, and maintaining a standard interface that allows application programs to be ported to different core processors.

One COTS+ method of achieving this is to implement a method of time slicing and to split applications into *strict tempo* and *scheduled* groups. Each strict tempo application is assured a specific amount of processing time in each time slice so that it can perform a certain number of defined algorithms in each allocated time slot. If its processing is completed in its allocated time, it will relinquish control to the next application. If an application overruns its time slot, it is timed out by the operating system. The scheduling provides sufficient time to each time slice for this to work efficiently. Hence, the addition of other schedule-level applications has no effect on the strict tempo

applications and merely causes the schedule-level applications to take longer. It is important to note that a strict tempo application may not be interrupted by a software interrupt. This is the reason for scheduling an application's interrupt process rather than vectoring the interrupt directly to the application.

The operating system will be capable of recognizing both periodic and aperiodic processes and scheduling and dispatching all processes. The operating system will provide status and fault data for each partition.

Since the operating system will need to perform with a high degree of integrity for critical applications, it may have unique certification criteria. It should therefore be as simple as possible.

The operating system also manages the allocation of logical and physical resources on behalf of the applications. It is responsible for the management of memory and communications. It receives interrupts associated with power failures and hardware error, relaying these incidents to the health monitoring function, which in turn directs the necessary actions to allow recovery or other actions. It will also channel application-specific software interrupts or events to the appropriate application and to a defined time scale.

As manager of all physical resources in this multiprogramming environment, the operating system monitors requests for resources and controls access to those resources that cannot be used concurrently by more than one application. It has access to all memory, interrupts, and hardware resources.

Fault tolerance, redundancy, and reconfiguration are inherent to the operating system. It will be capable of reporting faults and executing subsequent actions. The operating system software shall manage the redundancy within the core processor.

In allocating and managing resource requests and communication interfaces from and to applications, the operating system has limited controlled access to the application memory. The operating system monitors the hardware responsible for the integrity of the software partitions and communicates with a health monitoring function on software and hardware integrity failures.

The health monitoring function is specific to the core processor design and to the spacecraft installation. Therefore, it is recommended that this software be partitioned into an operating system health monitor and a recovery strategy table. The latter requires configuration definition and embedded recovery strategies.

The operating system contains an error reporting capability that can be accessed by applications. If an application detects a fault in the operation of the system, it is able to report this to the operating system, which in turn invokes the health monitoring function.

Applications may need to check system health and reconfiguration status for any reconfiguration that may have been performed.

The operating system is constrained by the APEX interface specification allow interchangeability of application software. A secondary aim is that it be constrained by the COEX interface specification to allow interchangeability of core hardware from different manufacturers. Specific hardware enhancements may be configured or added, and these features themselves may be a combination of both hardware and software.

It is recognized that combinations of applications vary in overall complexity. Simple applications may use only the basic features of a full operating system. The operating system may be designed to allow itself to be built to provide only those essential features or a full set of features. The configuration status of the operating system will then be available for applications to check compatibility.

It is also recognized that not all features of the operating system are available at the outset, and that some features will evolve. Again, the design of the operating system will allow this evolution, and, similarly, its version identification will be available as part of its build identification.

4.6.9 The APEX and COEX Interfaces

The COTS+ approach allows for the applications, operating system, and core hardware to be developed independently by separate manufacturers. For this approach to work, the interfaces require that rigorous standardization and detailed specifications be defined for each. The APEX interface is being defined in ARINC Specification 653. It is anticipated that these interface specifications may require updating as the technology progresses. Therefore, it is important to define the revision status of the interface specifications as part of system configuration management definition (see Subsection 4.6.11).

The APEX interface places rigid constraints on the operating system, application software, and to some degree, the entire system. Communication is standardized by making the format of all communications the same, whether the transfer is application to application or application to sensor/actuator. The APEX places layering and partitioning demands on the operating system to allow growth and functional enhancement.

Operating system requests, particularly communication requests, are made in one of several modes. Either the application can request that the function be performed and then suspended awaiting completion of that request, or that it continue running and either poll the status of the request or merely be alerted that the transaction is complete.

It is anticipated that the interfaces will be split into groups/areas such as memory management, data I/O, etc., and that each area will be further subdivided.

The processing of a communication request within the operating system consists of setting up the appropriate backplane bus format and passing the message to the hardware interface.

To ensure temporal determinism, each message definition includes a maximum and minimum time of response. Certain message types also include a timeout specification, which can be set up by the application. The response time can be calculated from the maximum and minimum delays of the backplane and network buses with an allowance for operating system processing. An operating system must meet this response time allowance. In this way, the interface specification constrains those functions that are time-dependent.

Hence all communications, including requests, commands, responses, and data I/O, between the applications and the operating system are processed by this rigorously defined message interface. Partitioning between applications and between applications and the operating system is controlled by standard hardware mechanisms. It can therefore be shown that if an application can be proved to be compatible with the APEX interface, it will interface correctly with the operating system.

The APEX interface is designed with full consideration for forward compatibility. Standardized operating system message definitions allow a growth path for future enhancements to the APEX interface. As long as any future APEX definition is a superset of earlier definitions, no conflict will arise as a result of any enhancement. A staged implementation is recommended.

The COEX interface specifies the hardware capabilities needed to support the operating system. These include initialization, memory management, bus interface, and interrupts.

It should be noted that application designers undoubtedly make assumptions about the response time of the operating system and hardware. Therefore, stringent constraints are placed upon the response of the operating system and hardware to ensure that different suppliers provide components with a similar grouping of response times and that the response of COTS+ systems integrated from different components will behave as required. Otherwise, this time element could defeat the aim of interchangeability. At the same time, the scheduling method will be both consistent and deterministic.

4.6.10 The Health Monitoring Software Function

An OS health monitoring function resides with the operating system and interfaces to a recovery strategy table defined by the spacecraft designer or system integrator. This health monitor is responsible for monitoring hardware faults within the core module and functional faults within the operating system. This OS health monitoring function is a subset of vehicle Integrated Health Monitoring System (IHMS).

Hardware faults detected by the BITE system include memory and processor faults and faults with the backplane data bus interface. Any local hardware reconfiguration strategies are hardware implementation specific, will take place within the hardware or the hardware interface system, and will be transparent to the rest of the system. The fault will be reported to the central maintenance system. Some faults need to be reported and acted upon at a higher level; therefore, an interface between the BIT/BITE functions and the health monitor is specified.

Faults detected within the operating system will include application violations, communication failures with remote devices (i.e., anything over the backplane or network buses), and faults detected by applications and reported back to the operating system.

A recovery table is used to specify the action to be taken in response to the particular fault. This action is initiated by the health monitor and includes terminating an application and starting an alternative application, together with an appropriate level of reporting.

The recovery action is largely dependent on the design of the system. The health monitor shall determine the need for action and initiate the recovery process. The recovery action is largely determined by the architecture of the core module.

Faults detected by other applications, such as sensor errors, will be reported to the health monitor.

4.6.11 System Configuration Management

The ability to load software onboard the spacecraft means there is a need to control the compatibility between different software components or between software and hardware components.

The system configuration management function of the OS health monitoring software is responsible for checking the versions of software loaded against compatibility criteria. One criterion is to check the revisions of APEX and COEX used for developing the operating system and applications. Only those configurations deemed compatible by this function are executable.

Initially, in addition to compatibility criteria, the total configuration of the system requires definition. This encompasses applications, sensors, actuators, indicators, and so on. In addition, that definition requires flow down from the system level onto the physical components of the system, i.e., cabinet configuration, core module, remote data concentrators.

Providing these definitions at each level is essential to allow the monitoring functions of the health monitor to be performed and any necessary fault recovery strategies to be defined at the appropriate level.

The operating system must know how the applications are configured to perform the necessary installation, initialization, and channeling of communications.

4.7 Data Sources and Destinations

4.7.1 Introduction

Data sources can be defined as those avionics components that provide data to the avionics cabinet for computation. Sources communicate their data through the network data bus or through interface modules.

Data destinations or data sinks receive data as a result of computations taking place in COTS+. Destination equipment receives data from the network data bus or from interface modules.

This subsection describes data sources and components used to process data in the COTS+ architecture. It includes data originating in peripherals and directed to computing equipment, data originating in computing equipment that is directed to peripherals, and equipment that communicates through special-purpose interfaces.

4.7.2 Objectives

This subsection recommends guidelines for standardizing electrical interfaces used in transferring information between data sources and destinations to minimize the number of signal types. It also provides guidelines for standardizing interface equipment, either integrated in the avionics cabinet or contained in remote equipment.

4.7.3 Identification

Typical data sources are sensors, control panels, relays, test generators, program pins and other avionic subsystems. Examples include sensors, control units, and antenna units. Typical destination equipment includes actuators, displays, relays, test storage, antenna units, and other avionic equipment. Subsystems are generally classified as equipment located outside the cabinets. They generally communicate with the cabinet-mounted equipment through digital transmission links.

4.7.4 Signal Types and Characteristics

Signals transferred between the processors and the source or destination can be analog, digital. or discrete.

4.7.5 Network-Compatible Devices

Network-compatible devices are those sensors, actuators and data concentrators that communicate with the cabinets via the global data bus or network, e.g., the ARINC 629 data bus. Where it is cost-ineffective or physically impractical interface directly with a sensor, simple devices may be interfaced by being clustered around a remote data concentrator. A remote data concentrator is a device that can serve as a source of data to or a sink from several simple devices (refer to Subsection 4.7.6).

4.7.5.1 Availability Considerations—The availability requirements of network-compatible devices themselves are wide ranging. The availability of these devices in terms of integrity, redundancy, and deferred maintenance needs is governed by the criticality of the function with which the device forms an integral part. The method of providing that availability may be internal fault tolerance of conventional function-level redundancy.

The availability needs will be determined by analyzing the functions, their criticality, and the network architecture.

The maintenance needs of a network-compatible device will also determine its availability needs. Sensors/actuators may be located in inaccessible regions of the spacecraft or where their removal from associated equipment may cause considerable disruption and retest. The maintenance needs of these devices may range from "fit and forget," deferred, and scheduled to as-required maintenance.

4.7.5.2 Environmental Considerations—The design of network-compatible devices is determined by a wide range of environmental requirements. Some of the devices will be subject to extremely harsh environments such as vibration, fluids,

and electrical effects (e.g., FADEC, fuel management). Others will be subject to relatively benign environments and may be located in the cockpit or cabin areas.

4.7.5.3 Sensor Capabilities—Sensors may have different levels of intelligence. The maximum level would be the ability to interface to the global data bus or network and to provide signal conditioning, calibration, health monitoring, and buffering. The minimum level would provide sensor data in raw form. Increased intelligence within sensors is encouraged since it reduces the necessary data bus traffic between the sensor and the associated processor. An air data probe may provide pressure in global data bus form rather than raw encoded form.

Similarly, an actuator may embody its inner-loop control and lessen the cabinet processing burden. In spacecraft configurations that require intelligence, but where it is impractical to provide that within the actuator itself, a remote data concentrator may perform that task on its behalf, together with intelligence for other sensors/actuators. In such cases, and where the devices have different integrity needs, the remote data concentrator will offer sufficient functional partitioning so that integrity is not compromised. However, such partitioning may be more appropriately provided in other ways, e.g., where sensors of similar integrity needs are grouped around one remote data concentrator and those of another level of integrity are grouped around another remote data concentrator.

The depth of intelligence allows improved built-in-test capability and applies equally to individual devices and remote data concentrators. A minimum requirement is the ability to determine device health (failure or malfunction) as well as data path health.

4.7.6 Remote Data Concentrator

In general, remote data concentrators within the COTS+ architecture are network-compatible devices. The fundamental purpose of a remote data concentrator is to act as a bridge between peripheral devices located in remote areas on the spacecraft and the global data bus.

A remote data concentrator provides a means for peripherals that would otherwise require dedicated wiring to processing cabinets to be accessible via the global data bus. Consequential benefits include decoupling the physical location of the peripheral from the processing center and increasing accessibility of the peripheral's data to several functions without increasing wiring.

To reduce dedicated spacecraft wiring and make such peripherals accessible via the global data bus, a remote data concentrator placed in the proximity of simple peripherals concentrates that data from several sinks/sources onto the data bus.

4.7.6.1 Degrees of Sophistication—In its simplest form, the remote data concentrator function operates as a pure data gateway between a collection of peripherals and the global data buses. Therefore, it multiplexes data from actuators and sensors and demultiplexes data arriving from processing centers.

The provision of a remote data concentrator allows degrees of sophistication to be made available for sensors and actuators that would otherwise be impractical. System monitoring and BIT functions can be provided for peripherals if they are unable to provide these functions themselves. Thus, sensor status could be transmitted over the global data bus to allow further isolation of faults, with consequent benefits in diagnostics and maintenance. The standardization of sensor I/O interfaces also makes it easier to implement this capability.

When the remote data concentrator is operating as a pure data gateway onto the airframe data bus, the form of data emerging from it is dependent on the sophistication of the sensor itself. An unsophisticated sensor provides its data in raw form.

The remote data concentrator can provide a degree of sophistication on behalf of simple sensors and actuators. An example is data fusion of several sensors to provide a more functional form of data, such as true airspeed (TAS), in digital form from air data probes. In addition, data fusion could provide additional integrity checks on redundant sensors or parameters from an otherwise inoperative sensor by interpretation of other sensor data, thus providing a degree of fault tolerance. Similarly, the inner-loop control of an actuator could be provided where it is impractical to integrate into the actuator itself.

Such sophistication reduces data traffic along the global data buses and decouples higher, more complex functions from the physical characteristics of sensors and actuators by enabling standardization at the digital interface level.

4.7.6.2 Availability—The availability of a remote data concentrator, in terms of its integrity, redundancy, and deferred maintenance needs, will be determined as a result of an analysis of the configuration of the spacecraft peripherals and their criticality.

The method of providing those needs is not specified herein. Availability requirements result from individual design tradeoffs between internal fault tolerance and system redundancy. The design of any I/O within a data con-

centrator will take into consideration that it may gather data from many sensors on behalf of several functions with different criticalities.

In relevant cases, provision shall be made for partitioning of signals on a functional basis and allowing verification of data path and data source.

4.7.6.3 Design Aims—Remote data concentrators are subject to a wide range of environmental conditions, depending on their physical location. Each location determines the method of implementation for that particular remote data concentration function.

Factors that affect the internal implementation of the function are:

- Environmental, ranging from benign (cockpit) to harsh (engine/wing);
- Maintainability, accessibility, fit and forget, deferred, or scheduled maintenance needs;
- Location and space.

Therefore, the design goal is interoperability at the functional level rather than its internal implementation.

With greater degrees of sophistication, functions similar to those in traditional commercial IMA cabinets can emerge. Where they exist, the design guidelines for equivalent cabinet functions will be applied to the remote data concentrator. It is recognized, however, that the peculiar constraints applied to remote data concentrators may suggest that the physical implementation and packaging may be quite different.

The use of generic modules for remote data concentrators is encouraged.

C-2

Section 5
Technology Shortfalls and Needs

5.1 General

Technology shortfalls and needs are classified under three categories: needs, concerns, and technology gaps. Since COTS+ technology is assumed mature by definition, shortfalls and needs occur when COTS+ technologies do not fit top-down space application requirements. Differences in avionic requirements or COTS+ characteristics requiring further development are identified as needs. Difficult differences are considered concerns. Differences requiring significant involvement, time-lapse, or risk are identified as technology gaps.

5.1 Technology Needs

The following COTS+ technology needs were identified.

- The disparity in linear acceleration requirements is to be accommodated by requiring qualification of COTS+ products to additional acceleration testing.
- Commercial aircraft normally do not specify acoustic requirements. Under MIL-STD-810, equipment located in areas where noise levels are 130 dB or less do not require testing to noise environments. Therefore, acoustic qualification will be required for equipment installed in high-acoustic environments such as near engines.
- SEU recovery with error detection and correction (EDAC) mechanisms and latchup protection must be provided in subsystems.
- For extended-duration missions, a storm cell or equivalent must be provided to protect critical avionics from major upsets. A safe must be used for storing COTS+ avionics cold spares.
- COTS+ avionics must be qualified by analysis to ensure that there are no detrimental outgassing effects.
- The operating system software serves several major purposes in the COTS+ concept. Therefore, it is a goal that a standard operating system be defined for COTS+.
- Commercial products will have to be designed to withstand humidity and salt spray environments.
- The health monitoring function is specific to the core processor design and to the specific spacecraft installation. Therefore, it is recommended that this software be partitioned into an operating system health monitor and a recovery strategy table. The latter requires configuration definition and embedded recovery strategies.
- The applications/executive (APEX) interface requires a detailed specification.
- Any COTS+ equipment that may be operating in a partial vacuum during the ascent phase shall be proven by operation during the evacuation phase of thermal vacuum chamber testing.
- Standardization of the avionics functions or hardware components is insufficient to provide unambiguous application function interfaces. For example, new functions may be added at a later date. Requirements for an overall common application software environment are necessary to integrate the building blocks of avionic applications.
- From a software perspective, COTS+ is a functionally distributed system that encourages the integration of many software functions. Requirements must be provided to:
  - Manage the communication flows between applications and the data on which they operate within the system.
  - Provide control routines to be performed as a result of system-level incidents that affect spacecraft operation.
- As with any other element within the COTS+ architecture, unambiguous software environment interfaces are necessary, not only between the elements within the software architecture but also at the interfaces between software and other physical elements defined in COTS+.
- Within the COTS+ concept, the placement of functions and software applications is distributed among the network of processing centers. Several applications are hosted on each processing center. These applications may originate from different avionics sources and be integrated into the selected imple-

mentation of the core processing hardware. For applications of different software criticality, reliable software partitioning must be used to ensure fault containment between applications.

- To provide application-to-application and application-to-hardware integration, comprehensive specifications must be generated. These specifications must define fault-tolerant interfaces between each application and the hardware resources and define how hardware resources are made available.

- Requirements for software portability must be generated. Portability of application software requires interface standardization between application software and core processor hardware. This interface can be a combination of both hardware and software, representing a common environment for application software. It can clearly be divided into two areas of focus:

  - The logical method of resource management and intercommunication;

  - The means of mapping those logical methods onto the physical hardware.

- Configuration control procedures must be generated to demonstrate that all conditions necessary to satisfy certification and V&V requirements are also satisfied after modification.

- The configuration control procedures generated must be capable of identifying hardware and software configurations that are compatible and constitute a validated configuration. It may be necessary for the equipment design to incorporate safeguards to enforce compatibility.

- The COTS+ parts list applicable to a particular series of vehicles' lists will identify alternate parts that have been determined to be acceptable. This list may include interchangeable components specified by an ARINC characteristic supplied by different manufacturers. While this type of documentation has proved to be of significant economic benefit to the airlines, in the COTS+ concept, it introduces the problems of identification, change control, and modification status accountability necessary of a configuration control system. This issue must be addressed and resolved.

- At a minimum, COTS+ components in RDIs must have to be some space-qualified characteristics because they may not be installed in protected environments. This means that some COTS+ products will have to be ruggedized.

5.2 Technology Concerns

The following COTS+ technology concern was identified.

- A cost-effective means of providing reliable COTS+ operation in radiation environments for missions other than ETO must be explored. This includes a study of radiation hardening and shielding.

5.3 Technology Gaps

No COTS+ technology gaps were identified.

Section 6
Development Direction and Recommendations

6.1 Administrative Recommendations

This study emphasized the identification of COTS+ technical shortfalls and needs, although both administrative and technical shortfalls and needs exist. In the administrative realm, there are perceived needs to organize and administer further effort in the exploration of COTS+ in space. Sponsoring and establishing technology maturation programs and COTS+ engineering and standards committees are deemed necessary and are recommended for furthering COTS+ integration. Administrating to these needs is recommended.

A comprehensive COTS+ development plan is needed. The complex COTS+ infrastructure requires establishment of COTS+ program priorities, partitioning of numerous tasks (software, hardware, networks, qualification testing, configuration control), and a schedule commensurate with levels of desired integration and funding. However, before this plan is initiated further assessment and analysis of unresolved study issues should be completed. It is beyond the scope of this study to recommend such a plan at this time. Transitional COTS+ integration, described below, is recommended for inclusion in the development plan.

6.2 Technical Direction and Recommendations

The COTS+ concept looks attractive. This study showed that COTS+ components and technologies are feasible in space applications. However, onging studies and technical development are recommended to answer unresolved questions and further explore the COTS+ concept.

The following development directions and recommendations are suggested for study. They provide additional detailed explorations, refine assessments, and provide means to resolve technology issues, needs, and concerns.

This assessment must further evaluate the physical partitioning architecture presented in this study. The alternative to the partitioning architecture is to employ ruggedized, hardened components that are able to withstand environments without the protection provided by partitioned areas. Because it requires 7.1 pounds to place each pound of payload destined for Mars in low-earth orbit using a cryogenic engine [RAFT91], a comprehensive cost/weight tradeoff study is required. This study is necessary to assess the cost-effectiveness of using various levels of COTS+ ruggedizing and hardening. The evaluation must include an assessment of all missions and various vehicles and engines.

6.2.1 Comprehensive Assessment

It is recommended that the COTS+ concept be tested for a complete vehicle architecture incorporating COTS+ as well as space-qualified subsystems. Assessments using quality function deployment (QFD) and analytic hierarchy process (AHP) metrics are recommended to properly evaluate the utility of COTS+ in space. These tools are very effective and provide a means to compare configuration characteristics such as power, weight, reliability, and cost to weighted evaluation criteria.

6.2.2 COTS+ Deferred Maintenance Study

It is believed that a study of opportunity costs, payload losses, and catastrophic losses will favor a COTS+ deferred maintenance concept. The concept is especially appropriate for expendable launch vehicle avionics using low-cost COTS+ components. This study, which emphasizes opportunity costs and channel replication for dependability, is recommended to resolve COTS+ cost utility questions [SPAC91; WENS90].

6.2.3 Transitional Integration

The COTS+ concept represents a step in avionic design philosophy for space avionic systems. It is recommended that implementations of COTS+ be incorporated in transitional stages to reduce the technical and economic risk for each space vehicle. It is hoped that the application of COTS+ can be fully achieved over a number of years as new spacecraft and spacecraft model derivatives are introduced and as confidence in the COTS+ concept grows.

Each step should represent an improvement in the overall avionics suite in accordance with the goals set for COTS+. As in many technology transitions, the benefits of the initial steps may not seem to offset the development cost and the risk if viewed in a narrow, first-cost analysis. The transition plan for full COTS+ implementation should therefore be viewed in its entirety. The first development of the initial COTS+ implementation should be viewed as an investment in the future.

If the orderly transition into COTS+ is shunned for reasons of first cost, disorganized de facto integration may evolve and result in increased equipment cost and certification

complexity. This will likely prohibit the growth in the contribution to overall spacecraft performance and efficiency promised by the COTS+ approach.

6.2.4 Other COTS+ Applications

Although this study investigates the use of COTS+ in space missions, COTS+ integration within ground-based systems or applications is also appropriate.

6.2.5 Maintenance Study

A maintained system COTS+ concept will offer considerable reliability improvement for the LTV/MTV and excursion vehicles over nonmaintained systems. Further COTS+ reliability and maintainability study is recommended to assess this concept, establish baseline channel reliabilities, and determine spares requirements.

Section 7
Notes

7.1 Definitions

Ada—The Ada programming language standard defined by ANSI/MIL-STD 1815A.

Application—That software consisting of tasks or processes that perform a specific avionics function on the spacecraft.

Availability—The expected probability that a system or piece of avionics equipment will be in an operational state.

Backplane—The physical circuit card and components consisting of the electrical connection points for interfacing cabinet resources to the outside world and integrating avionics modules.

Backplane Data Bus—a. The portion of the physical backplane that is dedicated to transferring data between modules internal to an avionics cabinet. b. The logic and protocol (network and data link layer) functions of the data bus used to integrate modules in the cabinet.

Best Commercial Practice—Government-sponsored new or modified designs that will not stand up to military environments but are solid enough to withstand civilian duty.

Bus Bridge—A module or function of a module that transfers data between data buses of the same format (e.g., FDDI to FDDI).

Cabinet—The physical structure used in IMA to provide an environmental barrier and house the avionics modules, cabinet resources and avionics backplane.

Civil Market COTS—Commercial products that are bought exactly as found in the civilian market and are allowed to flow with the changes and updates the vendor provides his customers.

Common Element—Those shared resources in the avionics cabinet that include the core processing module(s), I/O modules, LVPSs, and backplane.

Common Mode Failure—A failure occurring in common elements that tends to cause simultaneous failures in associated elements.

Computer—A device or group of devices that performs a data processing function.

Confidence—The extent that a combination of formal validation, verification, and analysis render a system or unit suitable for service.

Core Processor—A module that contains at least the processing resources and memory.

Core Software—All software and firmware in a core processor that is not part of the application process.

Coverage—A measurement of the ability of a fault tolerance mechanism to detect faults; expressed in percent.

Critical—A failure (or loss of component/function) that is likely to cause injury to persons or significant damage to material (IEEE).

Data Concentrator—A component that collects various types of data on the vehicle and outputs that data on global buses. A data concentrator is equivalent to a smart sensor.

Deferred Maintenance—Maintenance performed at a later, more convenient time and place after the identification of a failure. This corresponds to "fly with failure" for ELVs.

Deterministic—The property of software to produce a predictable outcome based on the preceding operations. Usually, the outcomes occur in a specified period of time with some degree of repeatability.

Dissimilar—In software, the intentional deviation in design method with the goal of producing the same result. This is often used to reduce the impact of generic faults in a design and therefore improves overall system integrity.

Essential—A function or component other than critical that is likely to reduce the ability of a more complex item to perform missions.

Event Driven—The occurrence of an asynchronous discrete action that causes a resultant action.

Executive Software—The software resident in the core processor that is responsible for scheduling and dispatching all application software, performing memory management, processing interrupts and has a standardized interface to the application programs.

Fail Operational—The property of a system that enables it to continue uninterrupted operation in the event of a failure.

Fail-Passive—The property of a system that recognizes that a failure has occurred and transitions the system into a passive state to avoid adverse affects on system operation.

Failure—The inability of a system to perform a required function or functions. A failure is the functional performance deficiency resulting from a fault. a. *Hard Failure*: A failure that has existed continuously since its occurrence. b. *Intermittent Failure*: A failure that occurs for a limited time, after which the functional ability recovers.

Fault—A fault is a physical condition that causes a device, component, or element to fail to perform in a required manner.

Fault Containment—To ensure that all faults are isolated to an individual LRM for maintenance action.

Fault Detection—The ability to positively identify that a fault has occurred.

Fault Isolation—The ability of a system to identify the location of a fault once the fault has occurred.

Fault Propagation—The inducement of a fault into devices other than the device in which the fault originated.

Fault Tolerance—The built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults (IEEE).

Fault Tolerance Renewal—Returning a fault-tolerant component to a completely operational state.

Function—A function is equivalent to a subsystem (e.g., autothrottle, autoland) and generally requires both hardware and software in its implementation.

Gateway—A module or function of a module that converts data from one data bus format to another (e.g., FDDI to High-Speed Data Bus).

Generic Fault—Those faults occurring primarily as a result of a flaw in the specification or design of a system and therefore tending to surface in any implementation.

Global—Of or pertaining to the spacecraft.

GLONASS—Global navigation sensor system developed by the Union of Soviet Socialist Republics.

Hard Failure—Those failures that are nonrecoverable and generally require a maintenance action.

Integrated Health Monitoring—An automated means of verifying the operational status of all critical hardware associated with vehicle assembly, launch, and support phases of operations. IHM is able to verify initial subsystem fault-free status, detect abnormal performance and impending failures, and identify suspected components.

Integrity Goal—A target based on statistical analysis that describes the operational, performance, and reliability objectives of a system.

Latent Failure—Failures that tend to occur without detection and have the potential to manifest themselves at a later time.

Memory Management—The property of the core processing module to allow system memory to be partitioned in a way that different application software can share mass memory devices without interaction.

Module—a. *Hardware*: A component whose packaging conforms to packaging concepts for integrated modular avionics. b. *Software*: A functional grouping of program statements to perform a specific process or task.

N-Version Programming—The practice of using multiple dissimilar versions of software to perform the same task for the purpose of improving system integrity.

Network—The integration of information associated with digital communication systems.

Olive Drab Commercial—Militarized products developed by commercial vendors at their own expense. The government has no control over the specifications or product delivery schedules.

Operating System—That portion of core software that includes the executive software and the software that constitutes the application executive and core executive interfaces.

Partition—a. An architecture concept that ensures the electronic separation of avionics functions so that a fault in one function cannot affect another. b. In software, that portion of code dedicated to a specific application. It usually depends on the use of memory management hardware to prevent inadvertent corruption of adjacent memory space.

Probabilistic—The property of software to produce a predictable output based on the statistical analysis.

Process—A programmable unit contained within a partition that executes concurrently with other processes of the same partition. A process is the same as a task.

Processor—A device used for processing digital data.

Random Failure—An uncorrelated failure of a hardware component.

Reconfiguration—The ability for equipment to automatically use alternate resources, logic, or computing paths in the case of a failure so as not to interrupt system operation.

Recovery Block—A portion of software dedicated to fault recovery that is executed in the event that a fault occurs.

Reference Vehicle—A future manned mission vehicle, platform, or module used to integrate COTS+ architecture for different missions.

Reliability—The property of an avionics system or component to perform over a predictable time period; usually expressed as mean time between failure (MTBF).

Repeater—A function or device that retransmits data on the same type of medium without altering the data.

Router—An intermediate function or device used to interconnect physical networks without altering the protocol.

SAFEbus™—Fault-tolerant, high-speed backplane bus for the Boeing 777 airplane avionics.

Sensor—A measuring or monitoring device for real-time data.

Soft Failure—A failure that is automatically recoverable.

Standard I/O—A family of modular I/O modules that interface a cabinet through its intracabinet bus and provide the interface to external systems, sensors, and actuators.

Strawman Configuration—COTS+ avionic architecture applied to different reference vehicles.

Strawman Framework—Generic COTS+ avionic architecture that can be modified and applied to different reference vehicles.

System—Any group of components, modules, or subsystems describing an operational entity.

Task—A programming unit contained within a partition that executes concurrently with other processes of the same partition. A task is the same as a process.

Terminal—The protocol circuitry, memory, crystal oscillators, and serial interface module that make up a complete transceiver.

Validation—The process of evaluating software at the end of the software development process to ensure compliance with software requirements (IEEE).

Verification—a. The process of determining whether the products of a given phase of the software development cycle fulfill the requirements established during the previous phase. b. Formal proof of program correctness. c. The act of reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether items, processes, services, or documents conform to specified requirements (IEEE).

7.2 Acronyms and Abbreviations

ACAF	Airplane Crew Alerting Function
ACARS	Aircraft Communication Addressing Reporting System
ACMF	Airplane Condition Monitoring Function
ADIRU	Air Data Inertial Reference Unit
AEEC	Airlines Electronic Engineering Committee
AHP	Analytic Hierarchy Process
AIMS	Airplane Information Management System
AMLCD	Active-matrix liquid crystal display
AMU	Avionics Module Unit—The basic dimension of a hardware module as defined by ARINC Specification 650
APEX	Application/Executive Interface
ARINC	Aeronautical Radio, Inc.
ASIC	Application-Specific Integrated Circuit
ASRB	Advanced Solid Rocket Booster
ATCRBS	Air Traffic Control Radar Beacon System

ATN	Aeronautical Telecommunication Network
ATOPS	Advanced Traffic Operating System
AVPAC	Aviation VHF Packet Communication
BIT	Built-in test
BITE	Built-in test equipment
BIU	Bus interface unit
CDU	Color display unit
CMC	Central maintenance computer
COEX	Core/executive interface
COTS	Commercial off-the-shelf
COTS+	Commercial off-the-shelf (including ruggedized and militarized) equipment
CRT	Cathode ray tube
DMC	Display management computer
DME	Distance Measuring Equipment
EEPROM	Elecrically erasable programmable read-only memory
EFIS	Electronic Flight Instrument System
EICAS	Engine Indication and Crew Alerting System
EID	Electronic Instrument Display
ELS	Electronic Library System
ELV	Expendable Launch Vehicle
EMI	Electromagnetic interference
ETO	Earth to orbit
FADEC	Full-Authority Digital Engine Control
FBB	Flyback Booster
FDDI	Fiber Distributed Data Interface
FDIR	Fault Detection, Isolation, and Reconfiguration
FMEA	Failure Modes and Effects Analysis
FMEFIS	Flight Management, Electronic Flight Instrument System
GPS	Global Positioning System
HERF	High-energy radio frequency
HOL	High-order language
ICAO	International Civil Aviation Organization
IHMS	Integrated Health Monitoring System
IMA	Integrated Modular Avionics
INS	Inertial Navigation System
ISO	International Organization for Standardization
I_{SP}	Specific Impulse
I/O	Input and/or output
LAN	Local-area network
LCD	Liquid crystal display
LEO	Low-Earth orbit
LOX/LH_2	Liquid oxygen/liquid hydrogen
LRM	Line-replaceable module
LRU	Line-replaceable unit
LTV	Lunar Transfer Vehicle
MA	Modular avionics
MAT	Maintenance Access Terminal
MCDU	Multifunction Control Display Unit
MEL	Minimum equipment list
MGR	Miniature GPS receiver
MITS	Mars Integrated Transportation System
MMI	Man-machine interface
MO	Magneto optic

MOPS	Minimum operational performance standards
MPRAS	Multi-Path Redundant Avionics Suite
MTBF	Mean time between failures
MTBMA	Mean time between maintenance alert/action
MTBUR	Mean time between unscheduled removal
MTTR	Mean time to repair
MTV	Mars Transfer Vehicle
NASA	National Aeronautics and Space Administration
NDI	Nondevelopmental item
NSA	National Security Agency
OS	Operating system
OSI	Open Systems Interconnection (Interconnect)
OTV	Orbital Transfer Vehicle
QFD	Quality Function Deployment
RTCA	Radio Technical Commission for Aeronautics
SA	Selective availability
SAARU	Secondary Attitude Air Data Reference Unit
SARPS	ICAO Standards and Recommended Practices
SASSO	Space and Strategic Systems Operations
SCB	Self-checking buses
SCP	Self-checking pair
SEI	Space Exploration Initiative
SRU	Shop-Replaceable Unit
SSDC	Sensor and System Development Center
SSME	Space Shuttle Main Engine
SSTO	Single Stage to Orbit
STME	Space Transportation Main Engine
TBD	To be designated/determined
TDC	Technical Data Change
TM	Technical Memorandum, Test and Maintenance
V&V	Verification and validation

Section 8
References

[ADAM] J.H. Adams, Jr., and M.M. Shapiro, "Irradiation of the Moon by Galactic Cosmic Rays and Other Particles," *Science on the Moon*, pp. 315–327.

[AEEC91] Airlines Electronic Engineering Committee, "Design Guidance for Integrated Modular Avionics," Draft 8, 28 July, 1991.

[AIMS91/1] "AIMS Hardware Requirements Document: Volume I - Global Hardware Requirements," Honeywell Commercial Flight Systems Group, October 7, 1991.

[AIMS91/2] "AIMS Hardware Requirements Document: Volume II - Cabinet Hardware Requirements," Honeywell Commercial Flight Systems Group, October 7, 1991.

[ALBE90] J.H. Albert, D.G. Alyea, and J.E. Shearer, "Vehicle Health Monitoring System Study: VHMSS," Final Report for July 1987 to September 1990, Boeing Defense and Space Group, September 1990, p. 183.

[ALLD87] J.R. Allder, "Avionics for Future Expendable Launch Vehicles," The Aerospace Corporation, 1987, pp. 127–134.

[ARINC651] Aeronautical Radio, Inc., "ARINC Report 651 on Design Guidelines for Integrated Modular Avionics," Draft 8 of Project Paper 651, 1 August 1991.

[ARTE91] "Artemis - Final Presentation," Results of the Engineering Feasibility Study, NASA Johnson Space Center, September 1991.

[ASKE90/1] J.R. Asker, "Lunar Base, Mission to Earth Pace NASA's Space Strategy," *Aviation Week & Space Technology*, March 19, 1990, pp. 180–181.

[ASKE90/2] J.R. Asker, "NASA Design for Manned Spacecraft Draws on Soviet Subscale Spaceplane," *Aviation Week & Space Technology*, September 24, 1990, p. 28.

[ASKE89] J.R. Asker, "NASA Offers Five Alternatives for Landing Humans on Mars by 2018," *Aviation Week & Space Technology*, November 27, 1989, p. 30.

[ASKE90/3] J.R. Asker, "Station Exceeds Weight, Power, EVA Limits, But NASA Says No Major Redesign Needed," *Aviation Week & Space Technology*, July 30, 1990, p. 25.

[AUST] R.E. Austin, "Cargo Launch Vehicles to Low Earth Orbit," Advanced Avionics Technologies, NASA Marshall Space Flight Center, *Proceedings of the Space Transportation Avionics Technology Symposium*, Vol. 2, 1990, pp. 87–106.

[BAHC91] J.N. Bahcall, "The 1990s: The Decade of Discovery," *Physics Today*, April 1991, pp. 24–30.

[BAIL89] R. Bailly, "Survivable Fiber Optic Networks for Military Applications," SPIE Vol. 1173, Fiber Optic Systems for Mobile Platforms III, 1989, pp. 25–33.

[BAIL91] S. Bailey, "Workshop on the Concept of a Common Lunar Lander," July 1991.

[BANG85] E. Bangsund, J. Keeney, and E. Cowgill, "Application of Inertial Upper Stage (IUS) Equipment and Experience to Orbit Transfer Vehicles of the 90's," 36th Congress of the International Astronautical Federation, 1985.

[BEAR90] T. Beardsley, "Slow Boat to Mars: Can NASA get us to the red planet?," *Scientific American*, April 1990, p. 14.

[BELL89] T.E. Bell, "Next-Generation Spacecraft Control," *IEEE Spectrum*, December 1989, pp. 34-38.

[BIND91] A. Binder and W. Holdenbach, "Artemis Payload Planner's Handbook," NASA Lyndon B. Johnson Space Center, September 30, 1991.

[BOOT90] R.A. Booth, R.A. Flanagan, G.Q. Loo, and D.J. VanAlen, "Multi-Path Redundant Avionics Suite (MPRAS)," Final Report for June 1987 - February 1990, Boeing Aerospace and Electronics, February 1990, pp. 68.

[BROA91] W.J. Broad, "NASA Moves to End Longtime Reliance on Big Spacecraft," *New York Times*, September 16, 1991, p. 1.

[BUYI90] "Buying NDI - Non-Developmental Item Program," Office of the Assistant Secretary of Defense for Production and Logistics, October 1990.

[CHIL] M.A. Childs, "Integrated Communication Systems Architecture," IEEE Colloquim on Future Military Avionic Architecture.

[COAT90] A. Coates, "Surviving Radiation in Space," *New Scientist*, July 21, 1990, pp. 42–45.

[COHN88] M. Cohn, "A Lightweight Transfer Protocol for the U.S. Navy SAFENET Local Area Network Standard," *Proceedings of the 13th Conference on Local Computer Networks*, 1988, pp. 151–156.

[CONT73] "Controller, Space Shuttle Main Engine, Specification," RC1007 Procurement Specification, Rocketdyne, North American Rockwell.

[COVA90/1] C. Covault, "Exploration Initiative Work Quickens as Some Lunar Concepts Avoid Station," *Aviation Week & Space Technology*, September 17, 1990, pp. 36–37.

[COVA90/2] C. Covault, "Israeli Rocket Proposed to NASA for U.S. Commercial Booster Project," *Aviation Week & Space Technology*, October 1, 1990, pp. 100–101.

[COVA90/3] C. Covault, "Japan Designing Atlas-Class Rocket to Launch Lunar, Planetary Missions," *Aviation Week & Space Technology*, August 20, 1990, pp. 63–68.

[COVA89] C. Covault, "Shuttle Launch of Galileo Jupiter Mission Highlights U.S. Space Science Renaissance," *Aviation Week & Space Technology*, October 23, 1989, pp. 22–24.

[COVA90/4] C. Covault, "Soviet Manned Lunar Mission Plan Used Modified Soyuz Spacecraft," *Aviation Week & Space Technology*, January 8, 1990, p. 44.

[COVA90/5] C. Covault, "White House Approves Soviet Talks on Moon/Mars Exploration Initiative," *Aviation Week & Space Technology*, April 9, 1990, p. 24.

[CROS90] M.C. Cross, "Japan drops satellite programme under U.S. pressure," *New Scientist*, March 31, 1990, p. 26.

[DEFI88] "Definition of a Space Transportation Systems Cargo Element (Shuttle-C)," Requirements, Concepts, and Configurations Trades/Analyses - Configuration Selection, Martin Marietta Manned Space Systems, April 1988.

[DOHE91] R. Doherty, "Shuttle to fly with new solid-state computers," *Electronic Engineering Times*, February 25, 1991, p. 1.

[DORN91] M.A. Dornheim, "Improper Antenna Deployment Threatens Galileo Jupiter Mission," Aviation Week & Space Technology, p. 25, April 22nd, 1991.

[DOSS89] Mel Doss, "Comparison of Active Matrix LCD versus CRT Displays for Avionic Applications," Honeywell Commercial Flight Systems Group, 1989.

[FRAG91] J.R. Fragola, "A second look at launch system reliability," *Aerospace America*, November 1991, pp. 36–39.

[FREE89] D. Freeman, E. Bangsund, "Space Transportation," *Aerospace America*, December 1989, p. 66.

[FRIE91] T.J. Frieling, "Reviving Saturn 5 May be NASA's Best Option to Attain Heavy-Lift," *Aviation Week & Space Technology*, May 20, 1991, pp. 67–68.

[GANO85] J.K. Ganoung, "Present Status of U.S. Launch Vehicles and Future Prospects," AAS/JRS Space Exploitation and Utilization Symposium, 1985.

[GAVA90/1] H. Gavaghan, "America cuts its launchers down to size," *New Scientist*, March 31, 1990, p. 33.

[GAVA90/2] H. Gavaghan, "Japan may help U.S. to 'explore' Mars and the Moon," *New Scientist*, March 24, 1990, p. 23.

[GENE90] "General Technical Requirements for Electrical and Electronic Equipment," Rev. A, Boeing, December 1990, p. 280.

[GILM90] P.A. Gilmartin, "House Kills Funding for Moon/Mars Effort," *Aviation Week & Space Technology*, July 2, 1990, p. 28.

[GREE89] D.T. Green and D.T. Marlow, "SAFENET - A LAN for Navy Mission-Critical Systems," *14th Conference on Local Computer Networks*, October 1989, pp. 340–346.

[GRIF91] M.D. Griffin and J.R. French, "Space Vehicle Design," AIAA Education Series, 1991.

[GUBA90] B. Gubanov, "Energiya looks to Mars and beyond," *Aerospace America*, July 1990, pp. 66–73.

[HANA89] J.F. Hanaway and R.W. Moorhead, "Space Shuttle Avionics System," NASA SP-504, 1989.

[HEND90] B.W. Henderson, "Livermore Plan for Exploring Moon, Mars Draws Space Council Attention," *Aviation Week & Space Technology*, January 22, 1990, pp. 84–88.

[HEND91] B.W. Henerson, "Market for Military Computers Growing in Time of Tight Budgets," Aviation Week & Space Technology, May 27, 1991, pp. 56–58.

[HENR89] R.C. Henry, "Launches into Low-Earth Orbit Should be Economical, Routine," *Aviation Week & Space Technology*, November 27, 1989, pp. 93-96.

[HERB90] C.G. Herbella, J.C. Karas, and J.R. Nordstrom, "Multi-Path Redundant Avionics Suite," Final Report, General Dynamics Space Systems Division, January 1990.

[HERG90] R. Hergott, "Ariane 5 aims for the future," *Aerospace America*, July 1990, pp. 74–75.

[HORD85] R.M. Hord, "Handbook of Space Technology: Status and Projections," CRC Press, 1985, p. 287.

[HUDS85] G.C. Hudson, "Phoenix: A Commercial, Reusable Single-Stage-To-Orbit Launch Vehicle," Space Exploitation and Utilization Symposium, American Astronautical Society, December 1985, pp. 383–394.

[HUGH90] D. Hughes, "NASA Will Fly Computer Processor, Erasable Optical Disk on Space Shuttle," *Aviation Week & Space Technology*, January 15, 1990, p. 47.

[HUNT88] D.M. Hunten, et al., "Space Science in the Twenty-First Century: Imperatives for the Decades 1995–2015 - Planetary and Lunar Exploration," Task Group on Planetary and Lunar Exploration, Space Science Board, Commission on Physical Sciences, Mathematics, and Resources, National Research Council, National Academy Press, November 1988, pp. 1–111.

[ITEG90] "Integrating Space Station Elements is Key Challenge to Program Managers, Engineers," *Aviation Week & Space Technology*, March 12, 1990, p. 19.

[JAPA90/1] "Japan Begins $2.5-Billion Effort to Develop Freedom Station Module," *Aviation Week & Space Technology*, August 20, 1990, pp. 79–82.

[JAPA90/2] "Japanese Space Studies Focus on Stations, Lunar Bases, Launchers," *Aviation Week & Space Technology*, August 27, 1990, pp. 82–83.

[KERR91] R.A. Kerr, "Galileo Hits a Snag," *Science*, Vol. 252, April 12, 1991, p. 638.

[KETC86] W.J. Ketchum, "Orbital Transfer Vehicle Concept Definition and Systems Analysis Study - Final Report," Volume II, OTV Concept Definition and Evaluation, Book 3, Subsystems Trade Studies, General Dynamics Space Systems Division, December 1986.

[KRIS91] K. Krishen, "Advanced Technologies for NASA Space Programs" Space: A Call for Action, *Proceedings of the 10th Annual International Space Development Conference*, May 1991, p. 46.

[LEKU64] H.W. Lekuch, "Several Considerations for Environmental Testing Under Simulated

Space Environments," Manned Space Reliability Symposium, American Astronautical Society, 1964, pp. 49–100.

[LENO89] J.M. Lenorovitz, "European Industry Submits Proposal for Space Station Design/Development," *Aviation Week & Space Technology*, October 16, 1989, p. 22.

[LOZI90] G.E. Lozino-Lozinsky and V.P. Plokhikh, "Reusable space systems and international cooperation," *Aerospace America*, June 1990, pp. 36–40.

[MAGE90] "Magellan Switched to Safer Mode; Computer Faults Still Puzzle Controllers," *Aviation Week & Space Technology*, September 10, 1990, p. 30.

[MARS89] E. Marshall, "Space Station Science: Up in the Air," *Science*, Vol. 246, December 1, 1989, pp. 1110–1112.

[MCRD89] U.S. Marine Corps, "Non-Developmental Item Handbook," May 1989.

[MILH82] MIL-HDBK-246A, Program Managers Guide for the Standard Electronic Modules Program, September 3, 1982, p. 42.

[MILH78] MIL-HDBK-251, Reliability/Design Thermal Application, January 1978s, p. 695.

[MILL91] M.G. Millis, "Technology Readiness Assessment of Advanced Space Engine Integrated Controls and Health Monitoring," *Proceedings of Conference on Advanced Space Exploration Initiative Technologies*, NASA Lewis Research Center, September 1991, p.15.

[MILS85] MIL-STD-2165, Testability Program for Electronic Systems and Equipments, Department of Defense, 1985, p. 74.

[MILS88] MIL-STD-45662A, Calibration Systems Requirements, Department of Defense, 1988.

[MOHR86] G.W. Mohrman, "Orbital Transfer Vehicle Concept Definition and System Analysis Study," Vol. VII, Integrated Technology Development Plan, July 1987.

[MOON91] "Moon/Mars Synthesis Group to Urge Saturn 5 Rocket Engines for Heavy Booster," *Aviation Week & Space Technology*, April 22, 1991, p. 24.

[MORG89] D.R. Morgan, "Pave Pace: System Avionics for the 21st Century," *IEEE AES Magazine*, January 1989.

[MPRAS TM1] General Dynamics Space Systems Division, "Multi-Path Redundant Avionics Suite," Technical Memorandum No.1, 1989.

[MPRAS1] General Dynamics Space Systems Division, "Multi-Path Redundant Avionics Suite," Final Report, 6 April 1990.

[MPRAS2] Boeing Aerospace and Electronics, "Multi-Path Redundant Avionics Suite," Final Report, February 1990.

[MULT90] "Multi-Path Redundant Avionics Suite Universal Sensor Interface Unit," Preliminary System/Segment Prime Item Specification, Honeywell Systems and Research Center, April 6, 1990, p. 57.

[NACH85] D.S. Nachtwey, "Manned Mars Mission Radiation Environment and Radiobiology," Manned Mars Mission Workshop, NASA/MSFC, AL, 1985.

[NAKA85] I. Nakatani and J. Kawaguchi, "Development of Attitude Control System of M-3SII Rocket," Space Exploitation and Utilization Symposium, American Astronautical Society, December 1985, pp. 315–325.

[NASA91] NASA Lyndon B. Johnson Space Center, *Proceedings of the Workshop on the Concept of a Common Lunar Lander*, July 1991.

[NATI91] "National Aeronautics and Space Administration (NASA) Open System Architecture Study," Lockheed Sanders Inc., August 1991.

[OASD90] Office of the Assistant Secretary of Defense, "Buying NDI," October 1990.

[ORBI80] "Orbital Transfer Vehicle Concept Definition Study," Final Report, Vol. 4, Selected Concept Definition, Boeing Aerospace Company, 1980, p. 188.

[ORBI85/1] "Orbital Transfer Vehicle Concept Definition and System Analysis Study," Vol. I, Executive Summary, Martin Marietta, March 1985, p. 87.

[ORBI85/2] "Orbital Transfer Vehicle Concept Defintion and System Analysis Study," Vol. VI, Subsystems - GN&C/Avionics, Midterm Review, Martin Marietta, March 1985, p. 213.

[OSCA88] Office of the Specification Control , Advocate General of the Navy, "Handbook for Implementation of Non-Developmental Item Acquisitions," 6 June 1988.

[PANE90/1] "Panel Says Confusion Hampers Development of Safety Features in Space Station Design," *Aviation Week & Space Technology*, April 23, 1990, p. 23.

[PANE90/2] "Panel Seeks Competition of Navy, USAF Launchers," *Aviation Week & Space Technology*, July 30, 1990, p. 28.

[PAYT91/1] G. Payton and J.M. Sponable, "Designing the SSTO Rocket," Aerospace America, p. 40, April 1991.

[PAYT91/2] G. Payton, J.M. Sonable, "Single stage to orbit: Counting down," *Aerospace America*, April 1991, pp. 36–39.

[RADH90] "Rad-Hard/Hi-Rel Data Book," Harris Military & Aerospace Division, 1990.

[RAFT90] M. Raftery, "The Application of Commercial Airplane Avionics to Advanced Space Transportation," *Proceedings of AIAA Space Programs and Technologies Conference*, September 1990, p. 6.

[RAFT91] M. Raftery, "Space Avionics Architecture Definition Study - Final Report," Boeing, July 1991.

[RAYT90] "Raytheon redesigns VAX for space flight," *Design News*, April 9, 1990, pp. 35–38.

[SAUN91] R.S. Saunders, G.H. Pettengill, "Megellan: Mission Summary," *Science*, Vol. 252, April 12, 1991, pp. 247–249.

[SCOT41] W.B. Scott, "ALS Cost, Efficiency to Depend Heavily on Process Improvements," *Aviation Week & Space Technology*, October 23, 1989, pp. 41–43.

[SHAF90] J.R. Shaffer and H.D. Mathews, "Lunar Transportation Facilities and Operations Study," Final Report, McDonnell Douglas Space Systems Company, April 1990.

[SHAR90] K. Sharp, "Computer I/O: Something for every architecture," *I&CS*, July 1990, pp. 35–37.

[SIMO88] R. Simoncic, A.C. Weaver, B.G. Cain, and M.A. Colvin, "SHIPNET: A Real-time Local Area Network for Ships," *Proceedings of the 13th Conference on Local Computer Networks*, 1988, pp. 424–432.

[SMIT89] B.A. Smith, "USAF Cuts Vehicle Design Work on Advanced Launch System," *Aviation Week & Space Technology*, December 18, 1989, p. 112.

[SMIT88] R.A. Smith, F.E. Warnock, "Suggested Electronic Equipment Standards for Nuclear Weapons Environments," Naval Surface Warefare Center, p. 52, January 1988.

[SPAC84] "Space Station Program: Description, Applications, and Opportunities," NASA Space Station Task Force, March 1984.

[SPAC90] "Space Avionics Requirements Study," NAS8-37588-TD006, Task Report, General Dynamics Space Systems Division, October 1990.

[STAF90] L. Stafford and M.J. Rendine, "Zenith Star Launch System," *Aerospace America*, September 1990, pp. 40–43.

[SPEC90] "Specifications," *Aviation Week & Space Technology*, March 19, 1990, pp. 129–176.

[TANA85] N. Tanatsugu, R.E. Lo, D. Manski, and U.M. Schoettle, "A Study on Two-Stage Launcher with Air-Breathing Propulsion," Space Exploitation and Utilization Symposium, American Astronautical Society, December 1985, pp. 365–382.

[UM-A91] University of Minnesota, Aerospace and Mechanics, "Mars Integrated Transportation System (MITS)," Team I Final Report for USRA/NASA at Marshall Space Flight Center, Winter 1991.

[UM-B91] University of Minnesota, Aerospace and Mechanics, "Mars Integrated Transportation System (MITS)," Team II Final Report for USRA/NASA at Marshall Space Flight Center, Winter 1991.

[USAF22] United States Air Force, "The COTS Book," Guidebook to COTS use and procurement, Rev. 22.

[VISI90] "Visitors to Mars by 2011," *Machine Design*, January 25, 1990, p. 16.

[VOOR90] C. Voorhees and L. McKee, "Dynamic Testing of Space Structures," *Sound and Vibration*, January 1990, pp. 32–37.

[WALD90] M.M. Waldrop, "Asking for the Moon," *Science*, Vol. 247, February 9, 1990, pp. 637–637.

[WENS90] John H. Wensley and Don D. Uhrich, "Reliability and Cost Considerations for Launch Vehicle Avionics," *Proceedings of the 9th IEEE/AIAA/NASA Digital Avionics System Conference*, 1990, pp. 117–124.

[WILL90] M. Williamson, "Space in the 1990s - the promise and the hope," *IEE Review*, January 1990, pp. 37–40.

[ZUBR90] R. Zubrin and D. Baker, "Humans to Mars in 1999," *Aerospace America*, August 1990, pp. 30–41.

Appendix A
COTS+ Components and Technology

Contents

Advanced Avionics
Johnson Space Center

Commercial Products

Advanced Avionics
Johnson Space Center

Related COTS Products

- ✓ Integrated INS/GPS
- GPS/GLONASS sensor
- Hexad with IFOG backup
- Model-based central maintenance computer
- Electronic library system (ELS)
- ✓ Optical disk storage system
- Digital map
- Ground-based expert diagnostics system
- ✓ SAFEbus™
- ✓ Airplane information management system (AIMS)
- ASCM computer
- ✓ Flat-panel displays
- Smart sensors and actuators
- Pressure devices (air data)
- Collision avoidance systems

Airplane Information Management System (AIMS) for the Boeing 777

Advanced Avionics
Johnson Space Center

Advanced Avionics
Johnson Space Center

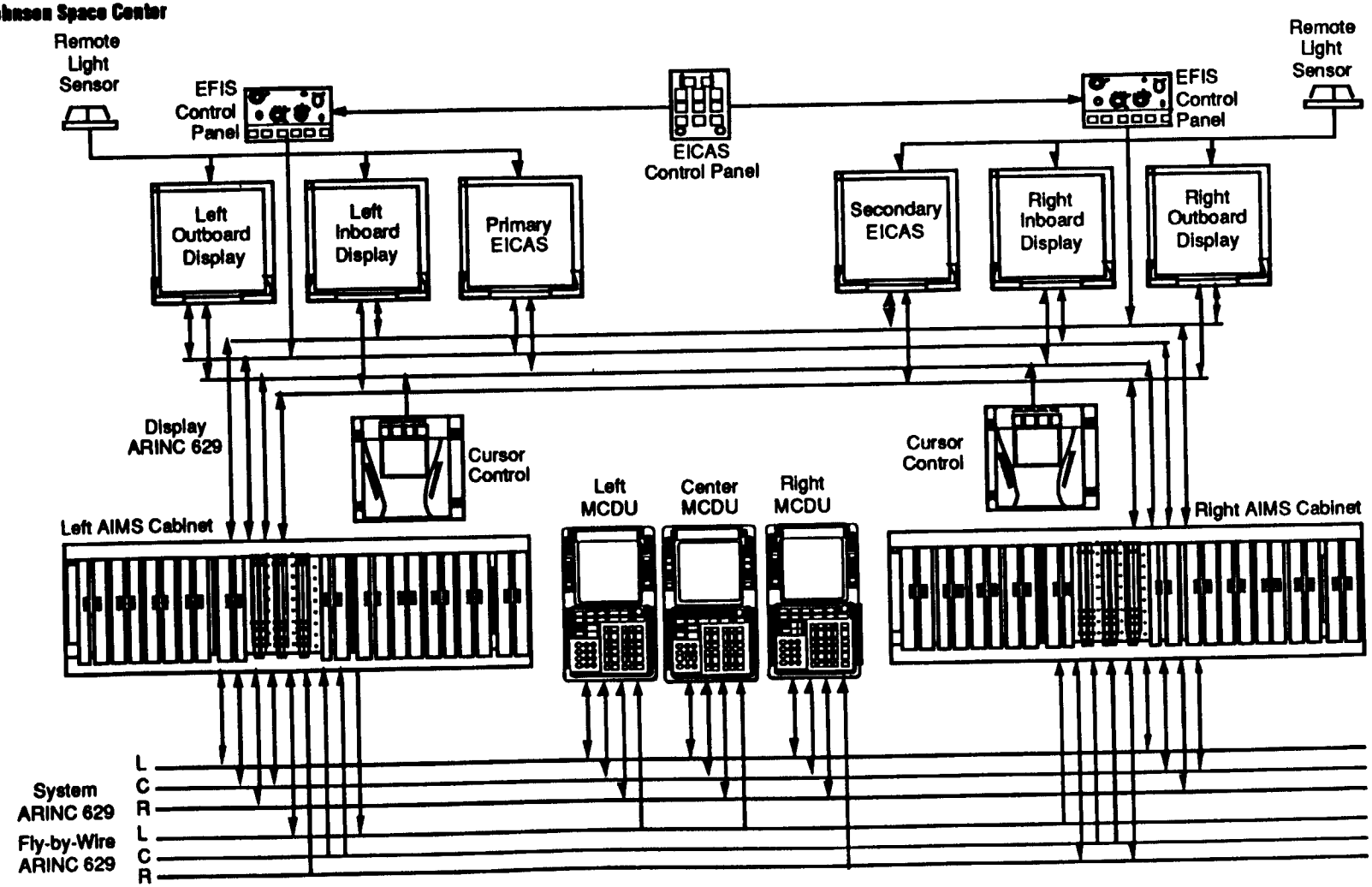
AIMS Architecture

Dual integrated cabinets provide processing and I/O hardware to perform the following functions

- **Flight management**
- **Displays**
- **Onboard maintenance**
- **Airplane condition monitoring**
- **Communication management**
- **Data conversion gateway**
- **Engine data interface**

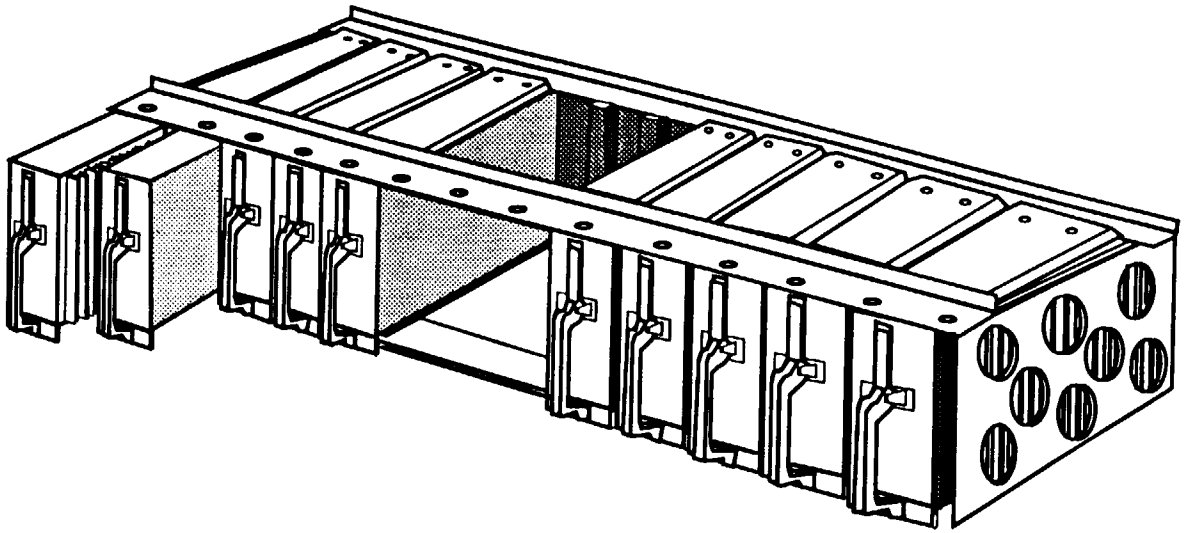
AIMS Architecture

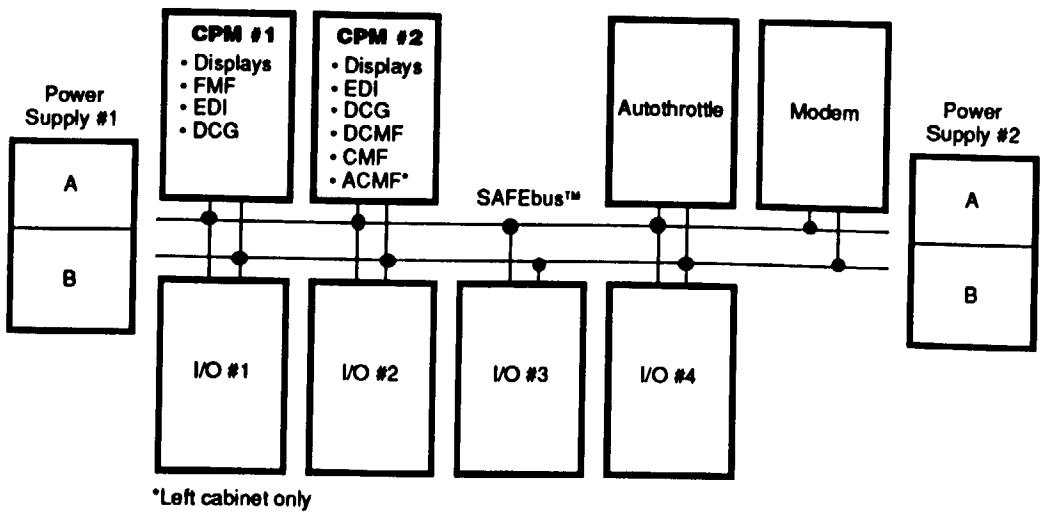
Advanced Avionics
Johnson Space Center



Honeywell

AIMS LRM Description

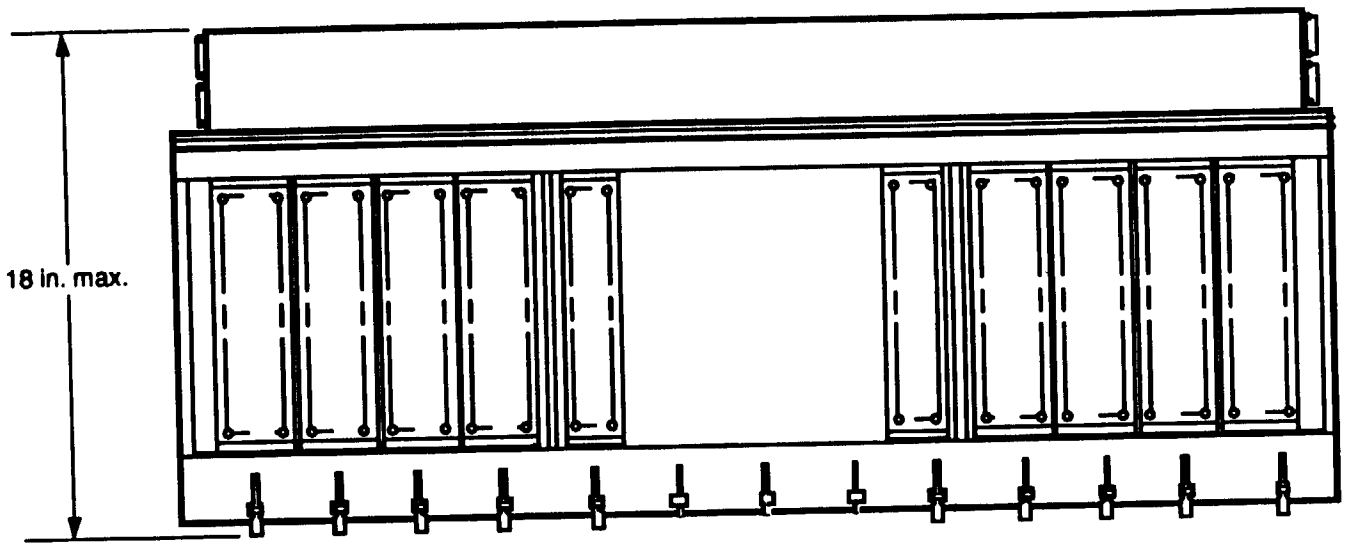




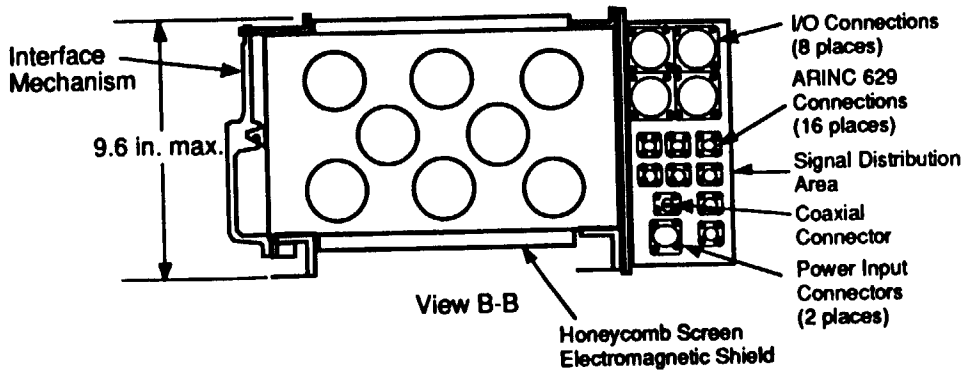
LRM Description	Quantity Required
Power supply	2
Processor	2
Standard I/O	4
Auththrottle servo	1
Modem	1
Chassis	0
Total	10

Cabinet Assembly Outline and Installation

Advanced Avionics
Johnson Space Center



View A-A



View B-B

- Current baseline module sizes are:
  - Power supply 3.65 in.
  - Processor 3.00 in.
  - Standard integrated optics 2.50 in.
  - Autothrottle servo 2.00 in.
  - Modem 1.50 in.
- Slot size flexibility provided by using movable guide rails
- Growth slots used for any size module (guide rail changes accomplished from cabinet front)

Honeywell

C910929-11

Systems and Research Center

Advanced Avionics
Johnson Space Center

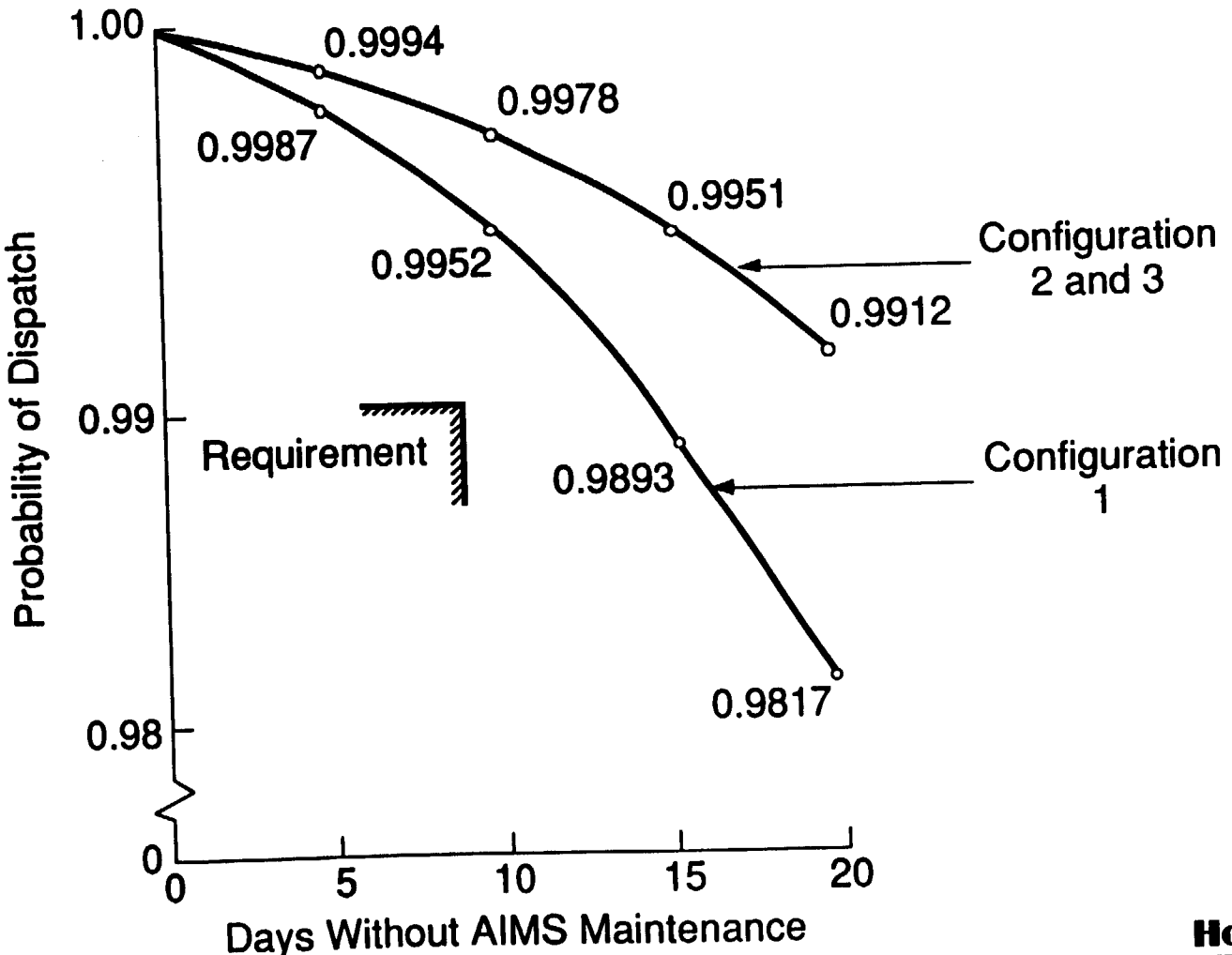
AIMS
Maintenance Design

- Hardware monitoring that provides
  - –Instantaneous fault detection/confinement
  - –Separation of hardware/software faults
  - –Transient fault suppression

- Built-in test bus
  - –Provides nonintrusive BITE logging path
  - –Supports industry standard diagnostic equipment
  - –Aids in shop "piece part" fault isolation (Level 3)

- Redundancy to allow maintenance-free dispatch for 10 days following any first failure

Probability of AIMS Dispatch vs. Time



Advanced Avionics
Johnson Space Center

SAFEbus™ Overview

Advanced Avionics
Johnson Space Center

Next-Generation Avionics Requirements

Key Drivers for Bus Development

- Robust partitioning
  - No failure in a function can cause another function to fail
    - -- Prevents resource hogging (processor or communications)
    - -- Prevents protection of public and private resources (program, data and I/O memories)
- Reliability
  - Aggressive no-maintenance policy requiring high-dispatch probability forces high reliability on all components
- Fault tolerance
  - No single failure can cause loss of essential avionics functions
  - Dispatch with failed components to meet dispatch probability requirements
- Flexibility
  - Must support many module types of differing capability
  - Must allow for addition/modification of cabinet functions without forcing recertification of unmodified functions
- Easy to debug and certify
  - Control of hardware/software integration
  - Predictable behavior over all possible operating conditions

Advanced Avionics
Johnson Space Center

SAFEbus™ Attributes

- Full concurrent monitoring
  - All transactions are performed dually
  - Dual monitoring at multiple points
  - Low-latency fault detection
  - Total fault containment of bus-related errors
  - Data is transmitted on two independent buses
  - 100% detection of single-bit transmission errors
  - No error coding overhead required
- Fault tolerant
- Decentralized control
  - Improves availability
  - Simple BIU synchronization scheme
- Supports multiprocessor architecture
- Debug modes

Advanced Avionics
Johnson Space Center

SAFEbus™ Attributes

- Table-driven protocol
  - –Assigns time slots to each message
  - –Eliminates arbitration
  - –Guarantees determinism, synchronization
  - –Issues real-time interrupts
  - –Synchronizes processors to I/O, other processors
  - –Anticipates partition data requirements
  - –Eliminates address transmission
- Increases bus efficiency
- Serial transmission
  - –Minimum pin count
  - –30 MHz worst case, growth options
  - –94% efficiency worst case
  - –64% spare with implemented growth

Advanced Avionics
Johnson Space Center

Avionics System Expandability/Growth Issues

Software Impact of Node Addition

- Bus-based systems are considered flexible and extensible (as opposed to nonbus systems). This virtue is true for hardware but not necessarily for software.
- Each addition of a device or function (node) to the bus involves different levels of software impact, depending on the bus scheme.
- It is estimated that software cost will be about 80% of future avionics data processing systems. So the attention should be focused on software issues.

Additions \ Access Control	Hybrid TDPA Bus	Central Control Bus	Contention Bus	Token Ring
Receive only	None	Change bus controller software,V&V all software in bus controller host, V&V system timing	None	V&V system timing
Noncritical transmit	None	"	None	V&V system timing
Critical transmit reserved	None	"	Impossible	One-time V&V of all possible system timing combinations
Critical transmit appended	Download new table	"	Impossible	V&V system timing
Critical transmit rescheduled	Download new table, V&V system timing	"	Impossible	V&V system timing
Spare	Download new table, V&V system timing	" (extensive)	Unreliable	V&V system timing for failed and unfailed

Honeywell

C910929-19

Systems and Research Center

Advanced Avionics
Johnson Space Center

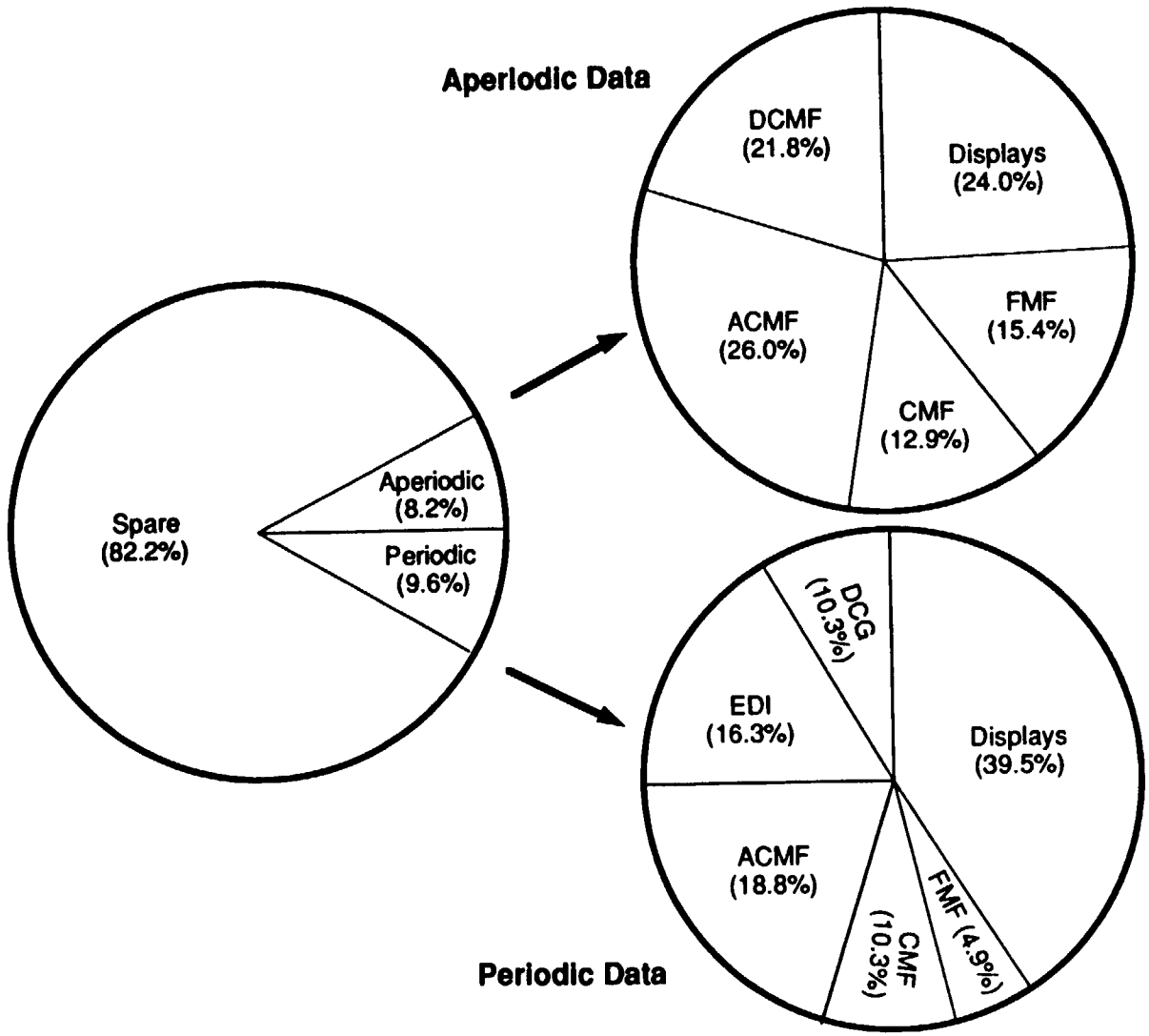
Backplane Buses

	SAFEbus	PI-bus	VMEbus	Futurebus
Data bits (options)	1 (2)	16 (32)	16 (32)	64 (128,256)
Signal/clock lines				
• Single bus	2 (3)	30 (47)	67 (107)	122 (186,314)
• FS	4 (6)	30 (47)	134 (214)	244 (372,628)
• FO/FS	8 (12)	43 (59)	201 (321)	366 (558,942)
• FO/FO/FS	8 (12)	73 (106)	268 (428)	488 (744,1256)
Throughput with 32-bit data (Mbyte/s)	3.5 (7)	5 (10)	12.9	15.5
Worst arbitration time (μs)	0	0.64	136.9	89.5
Clocks/strobes+	Source clocked++	Synchronous	Asynchronous**	Asynchronous**
Address space(s) (bytes)+++	$15 * 2^{20}$	$8 * 2^{128}$	$64 * 2^{24}$	$1 * 2^{64}$
Multiplexed	No	Yes	Yes	Yes
Memory protection	Yes	No	No	No
Time determinism	Yes	No	No	No
Fault tolerance built in				
• Bus lines, pins	Yes	Yes	No	No
• BIUs, drivers	Yes	No	No	No
• Buffer memory	Yes	No	No	No
Broadcast capability	Yes	Yes	No	Yes
Driver technology*	BTL	BTL	TTL	BTL
Backplane layers	1	4	6	>5
Extender card	Supported	Supported	Not specified	Supported
Live insertion	Yes	Yes?	No	Yes
Debugging	Easy	Moderate	Very difficult	Very difficult
Built-in system debug features	Yes	No	No	No
Designed for system validation	Yes	No	No	No

Notes:
FO = Fail operative, any bus line or pin, nonidentical faults.
FS = Fail safe, any bus line or pin, nonidentical faults.
*BTL is superior to TTL for backplane applications.
**Asynchronous buses are difficult to test and diagnose, conditions are not repeatable.
+Asynchronous buses are less well behaved in the face of meta-stability.
++Source clocking is the fastest method.
+++Address space(s) = number of spaces x number of bytes per space.

Advanced Avionics
Johnson Space Center

SAFEbus™ Growth



Honeywell

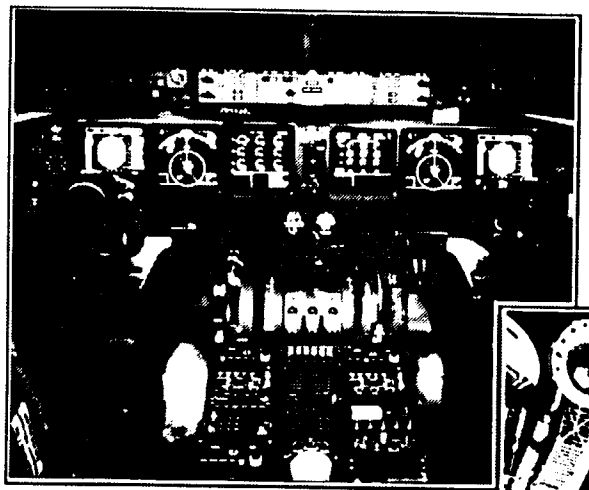
Advanced Avionics
Johnson Space Center

Flat-Panel Display System

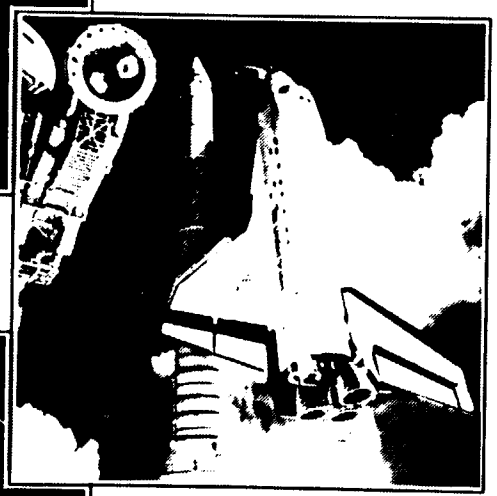
COTS FOR SPACE

Advanced Avionics
Johnson Space Center

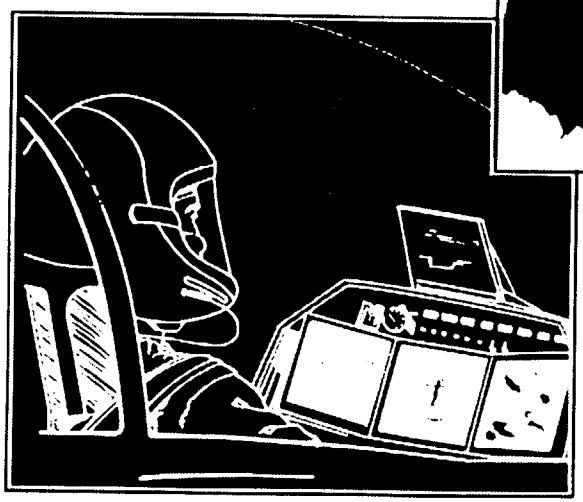
Flat-Panel Displays



Commercial



Space



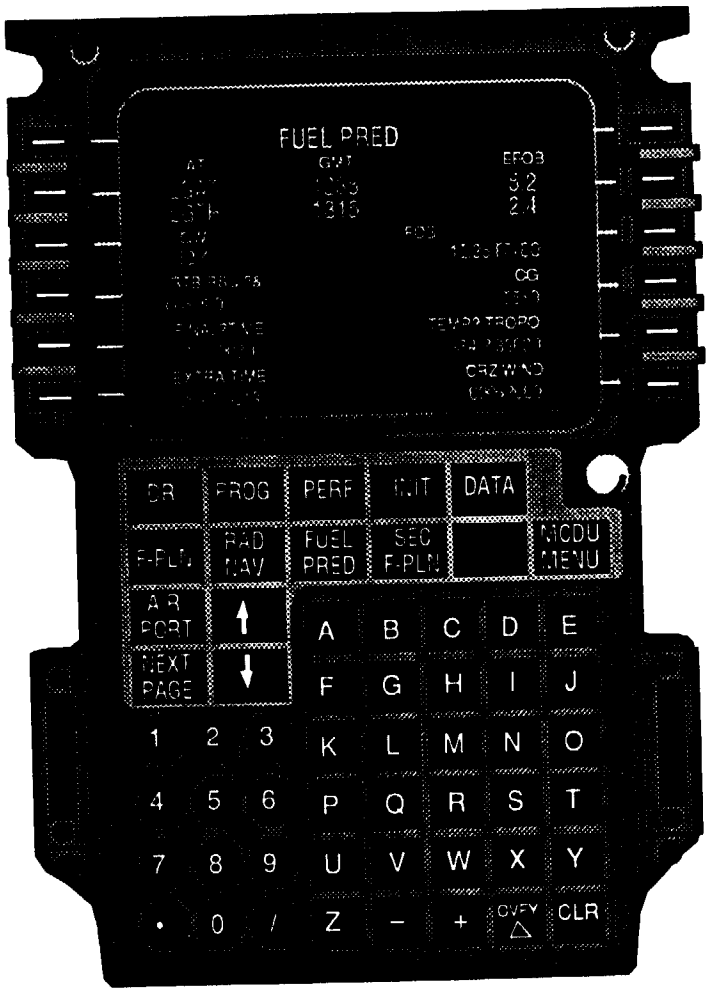
Military

Honeywell—the leader in full-color, high-resolution flat-panel display for future airborne and space applications

- **High reliability through integrated drivers**
- **Wide-angle, full-color gray scale**
- **Daylight readable**
- **Low power, weight, voltage, and volume**

Advanced Avionics
Johnson Space Center

Multifunction Control Display Units



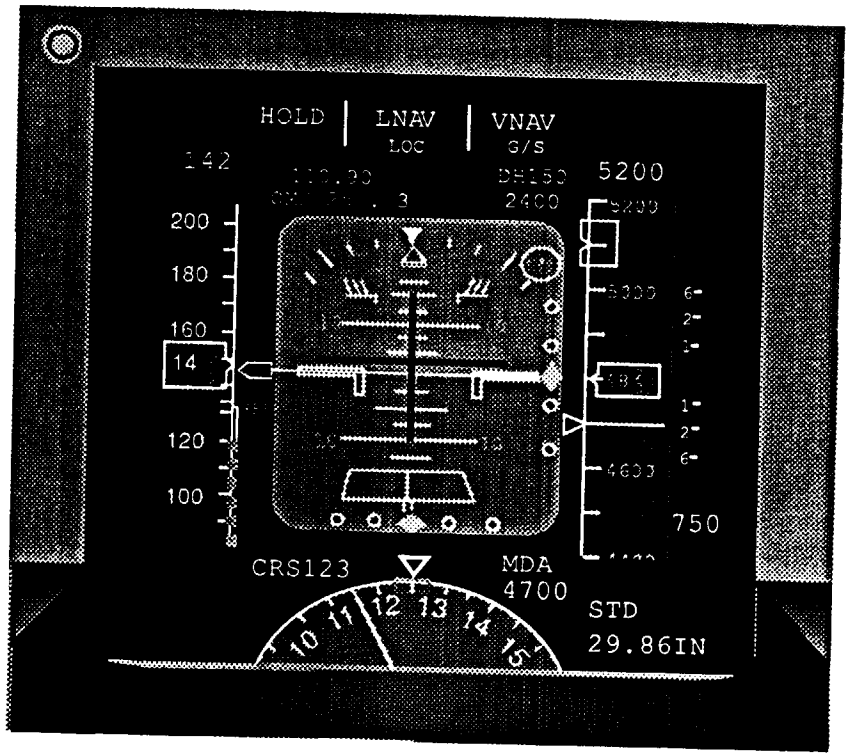
Honeywell

Systems and Research Center

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

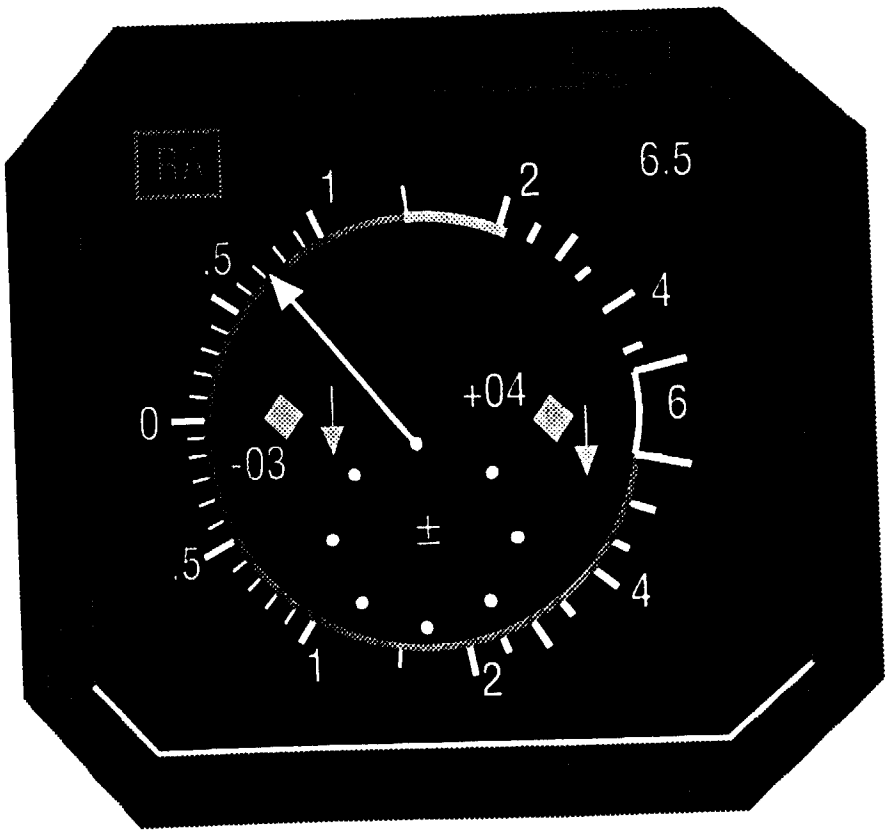
Electronic Instrument Displays



COTS FOR SPACE

Advanced Avionics
Johnson Space Center

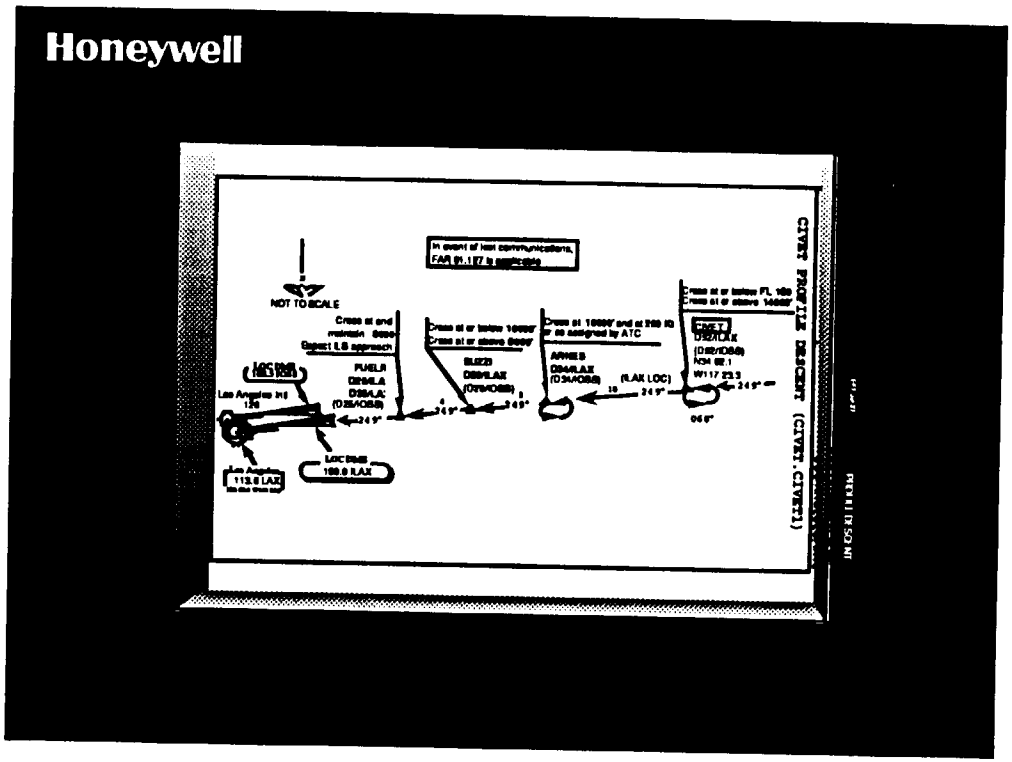
Integrated TCAS Displays



COTS FOR SPACE

Advanced Avionics
Johnson Space Center

Electronic Library System (ELS) Displays



Advanced Avionics
Johnson Space Center

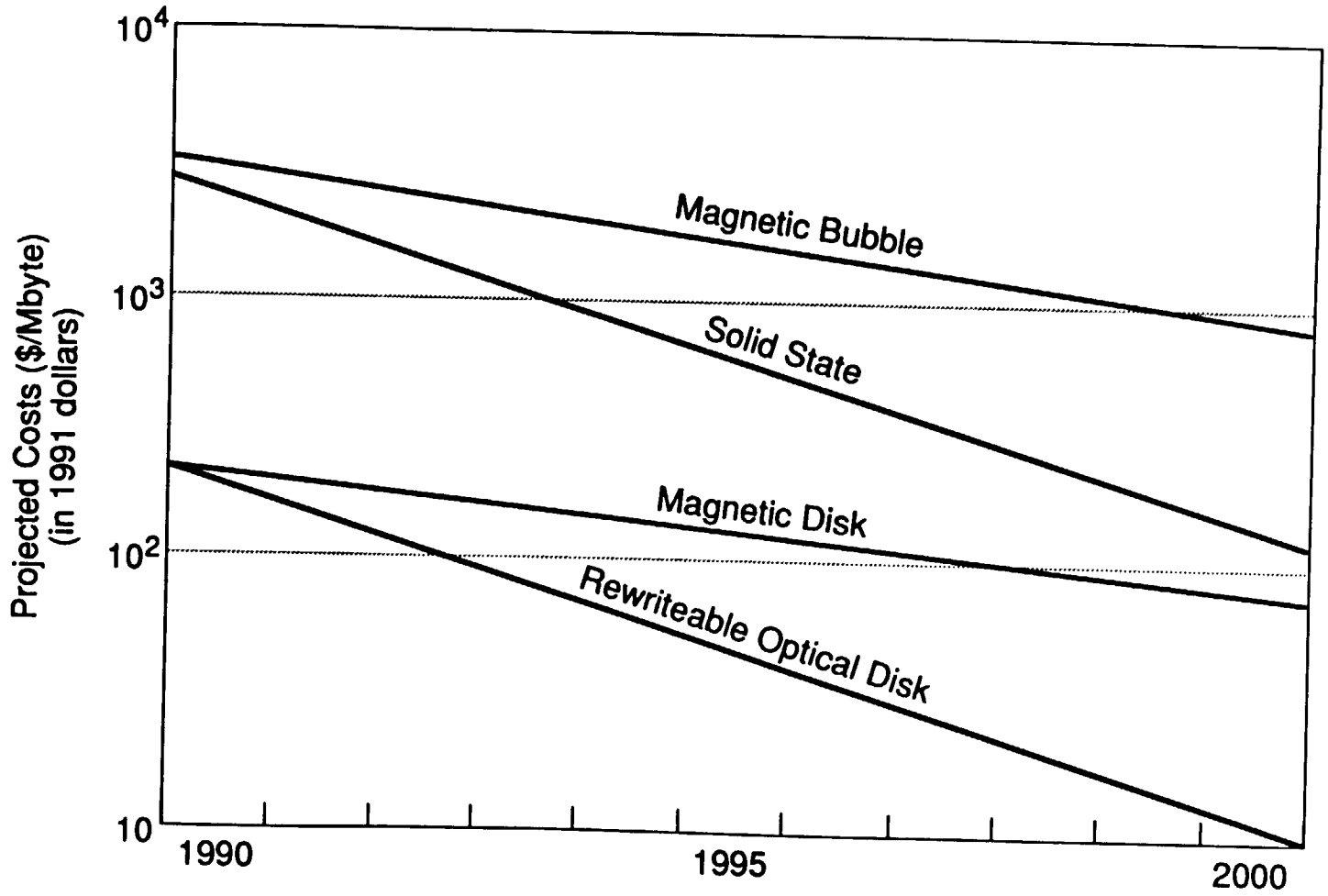
A-30

Optical Disk Storage System

COTS FOR SPACE

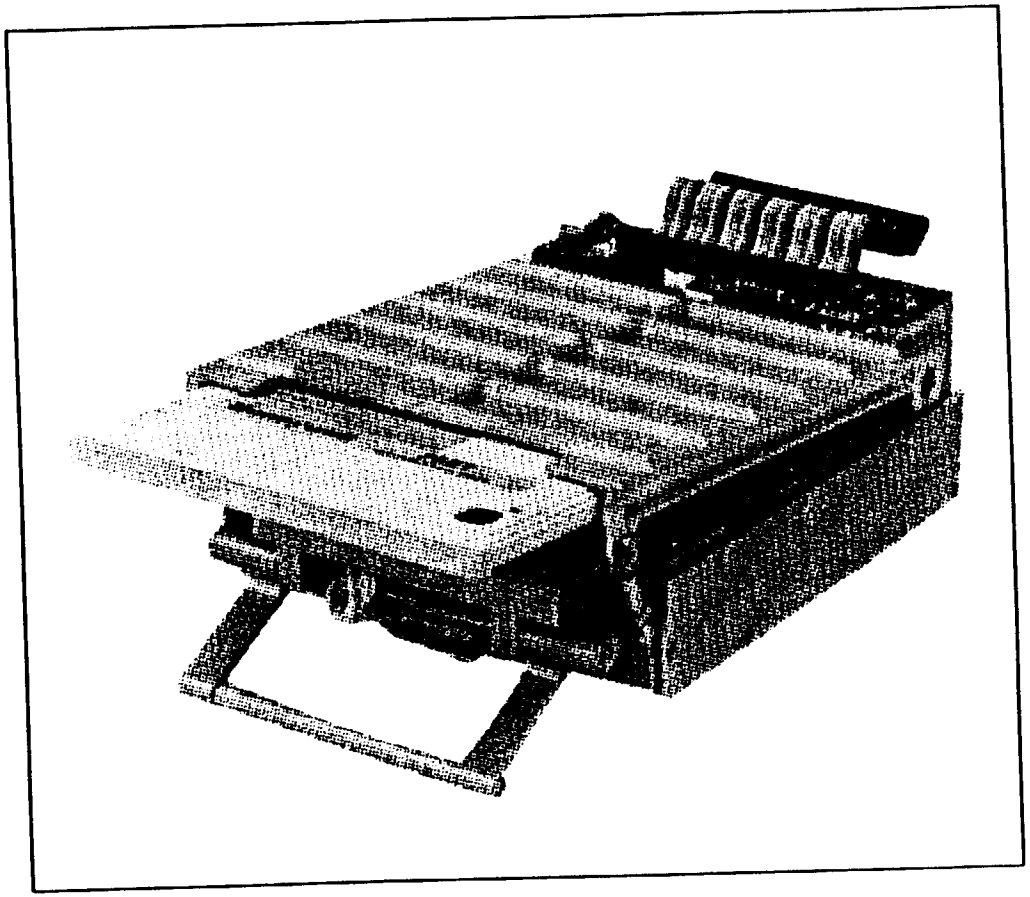
Advanced Avionics
Johnson Space Center

Projected Costs of Memory Technologies

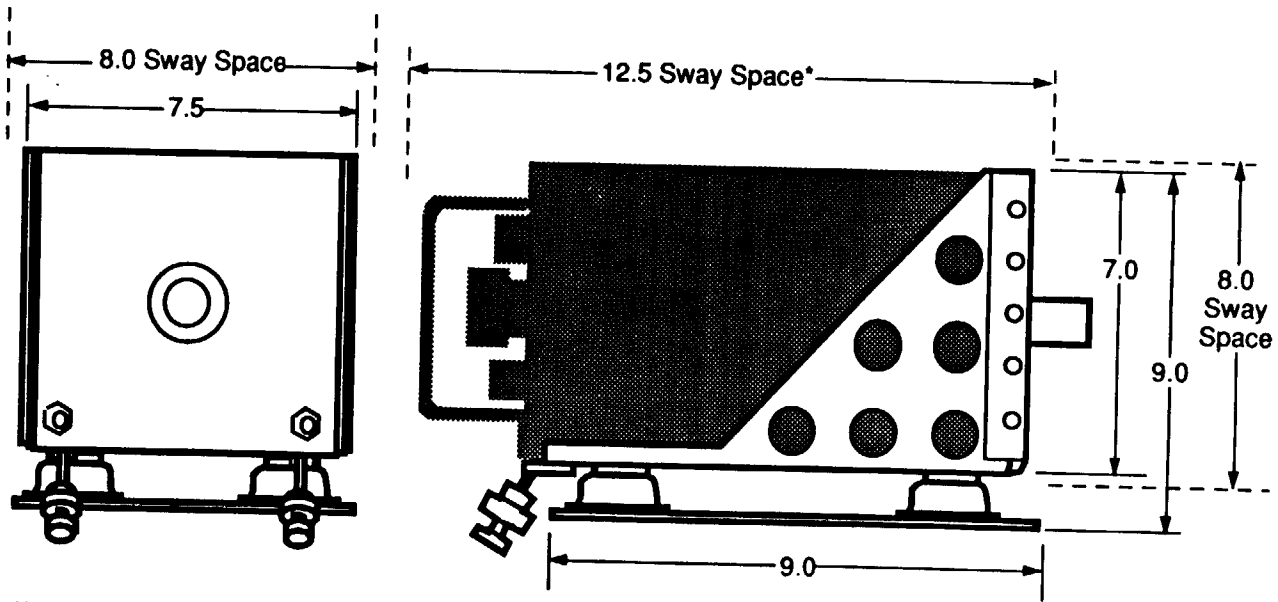


Optical Disk for Electronic Library and Mass Data Storage Functions

Advanced Avionics
Johnson Space Center

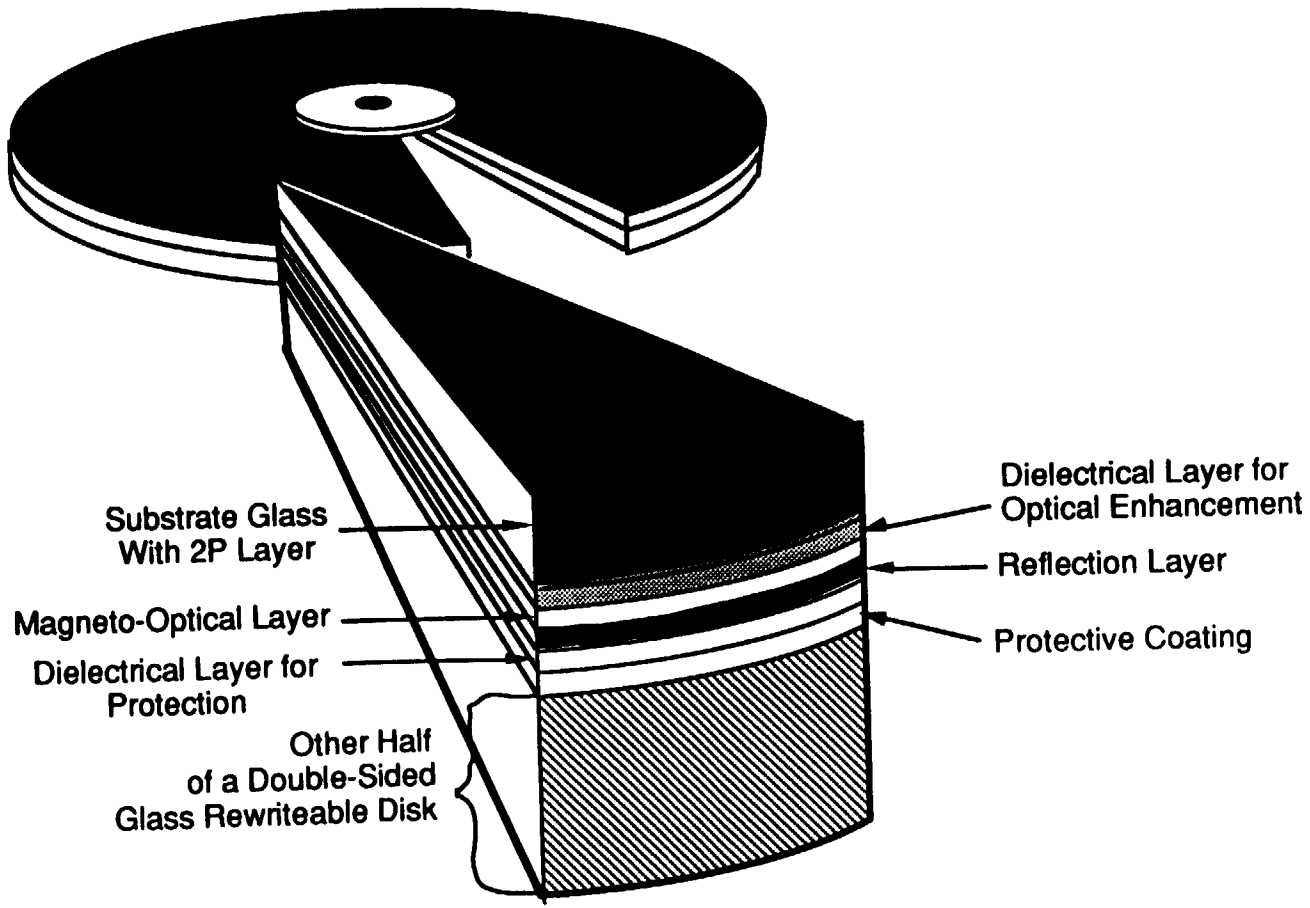


Optical Disk Memory Unit Mounting Tray



*Does not include mating connections
7.5 in. W × 9.0 in. H × 9.0 in. D

Magneto-Optical Disk Structure



Advanced Avionics
Johnson Space Center

Proposed Blue Laser Data Storage System Program

Program Goals

Performance: 2 Gbyte

Format: 5-1/4-in. disk

Environment: ambient test environment

Advanced Avionics
Johnson Space Center

Current Mass Data Storage Systems for Health Monitoring and Control

Mass Memory Unit (MMU)

- Digital magnetic tape
- 16 Mbytes

Modular Auxiliary Data System (MADS)

- Analog magnetic tape
- One week to distribute data

Technology advances required to improve health evaluation through increased capacity and functionality for quick access and analysis

Advanced Avionics
Johnson Space Center

Reusable Rocket Engines— Mass Data Storage Needs

Reusable rocket-engine evaluation drives need for reliable mass data storage

- STS
  - Three SSMEs
  - High performance, low design margin
  - Continual (re)evaluation for maintenance redeployment
- NLS (ALS)
  - Seven STMEs
  - Increased design margin, up to 15 missions
  - Between mission assessment need
- OTV
  - Four OTV engines
  - ICHM applied to extended-duration no-maintenance scenario
  - Post-firing prognostics may require on-vehicle MDS playback
  - Rewriteable media for subsequent missions

Advanced Avionics
Johnson Space Center

Reusable Rocket Engines— Mass Data Storage Needs

- Record parameters for post-use/reuse assessment
- Data interpreted for remaining life calculations

Advanced Avionics
Johnson Space Center

Reusable Rocket Engines—Mass Data Storage Needs

Considerations

- Capacity
  - Conventional instrumentation suite: temperature, pressure, accelerometer, flow, position, commands
  - Expandable to accommodate emerging technologies: pyrometer, ultrasonic flow meter, plume specification, visual, mass spectometry
  - Potential additions: record image data
- Rate
  - Analog-to-digital conversion pushes sampling rate
- Reliability
  - MDS record volume ≥ telemetry stream
  - Most exact available record
  - Redundancy required to ensure data record

Advanced Avionics
Johnson Space Center

Mass Data Storage Systems on STS

- Mass Memory Unit (MMU)
  - Flight operations recorder
  - IBM/Odetics magnetic tape digital recorder
  - Tape erased after successful telemetry

- Modular Auxiliary Data System (MADS)
  - Reconfigured magnetic-type recorder for analog data
    - -- Turbo pump
    - -- Gimbal bearing
  - Operates in crew compartment
  - Requires GSE to extract data
  - One week duration for data receipt at RD

Advanced Avionics
Johnson Space Center

Future Directions of Complex Sensing Systems

Addition of complex sensing systems will increase data recording demands

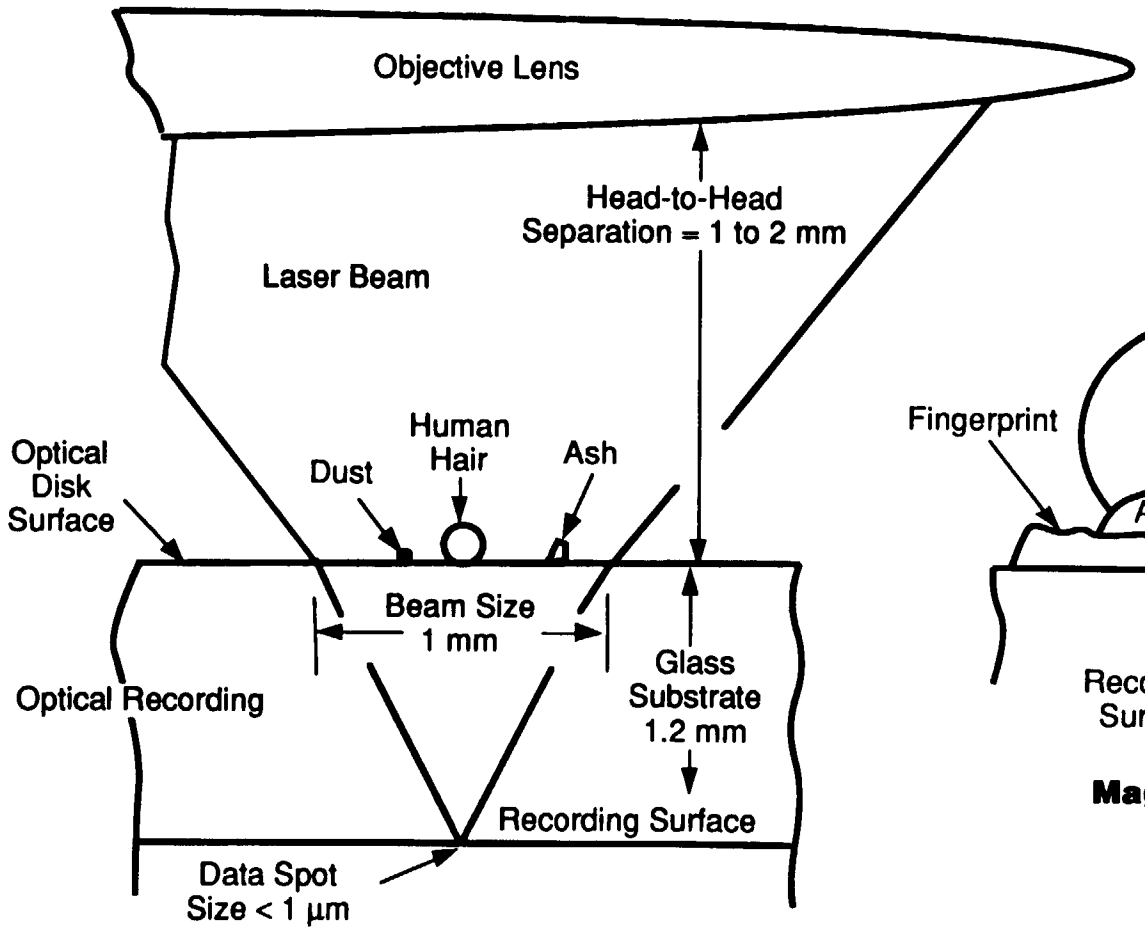
- Video-based systems
  - Plume spectroscopy
    - -- In-flight anomaly detection
    - -- Correlation with "standard" indicators
- Automated visual inspection
  - Pre-/post-use hardware evaluation
  - Miniaturization and robotics allow possible use on OTV-type missions
- Preflight, flight, post-flight leak detection
  - Mass spectrometry
    - -- Leak occurrence, composition identification
  - Optical leak detection
    - -- Leak occurrence, location determination

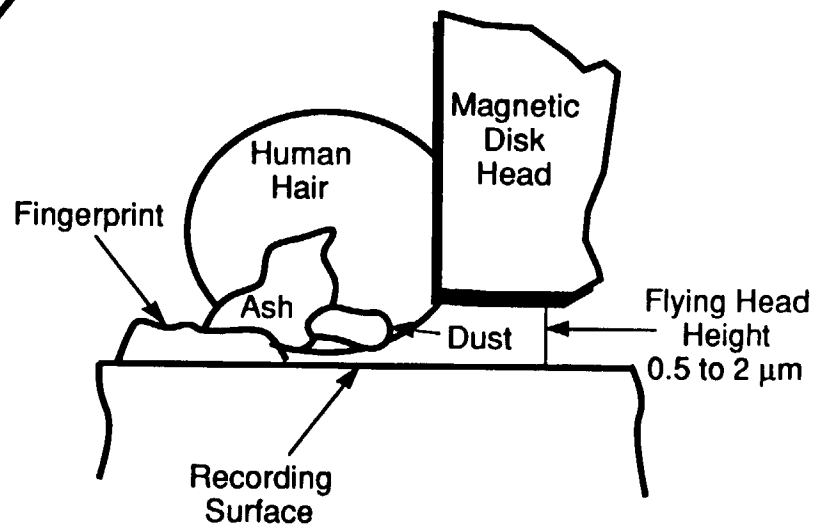
Advanced Avionics
Johnson Space Center

Advantages of Optical Storage

- Product medium is inherently rugged
  - Storage medium is shielded by protective glass
  - Large head/disk spacing
  - No head crashes
  - Superior performance in harsh environments
- Random data access
- Highest storage density, lowest cost per byte
- Airborne read-and-write capability
- Removable media
- Change audit trail (write-once technology)
- Reusable media (rewriteable magneto-optic technology)

Optical Recording Advantage





Magnetic Recording

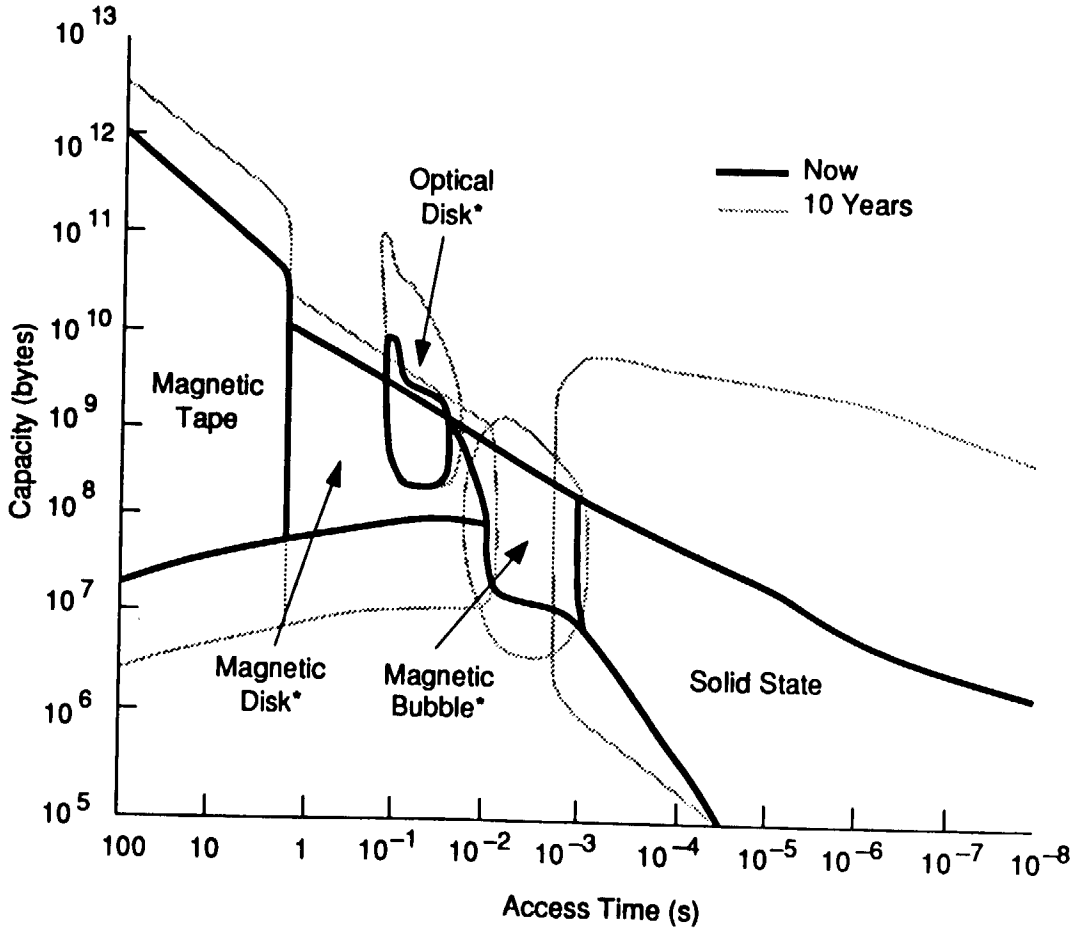
Advanced Avionics
Johnson Space Center

Mass Data Storage Technology Comparison

Technology	Advantages	Disadvantages
Optical disk	• Large data capacities • Removable cartridge size/cost • Ruggedness (head/media gap) • Low cost/Mbyte • Rad-hard and EMI-hard media	• Slow access time • Low data transfer rates
Magnetic disk	• Relatively large data capacities • Driven by commercial technology	• Ruggedness (head/media gap) • Removable cartridge size/cost
Solid state	• Semiconductor cost curve • Ruggedness • Fast access time • High data transfer rates	• Relatively low capacities • Very high cost/Mbyte • Removable cartridge size/cost • Radiation and EMI susceptibility

Honeywell

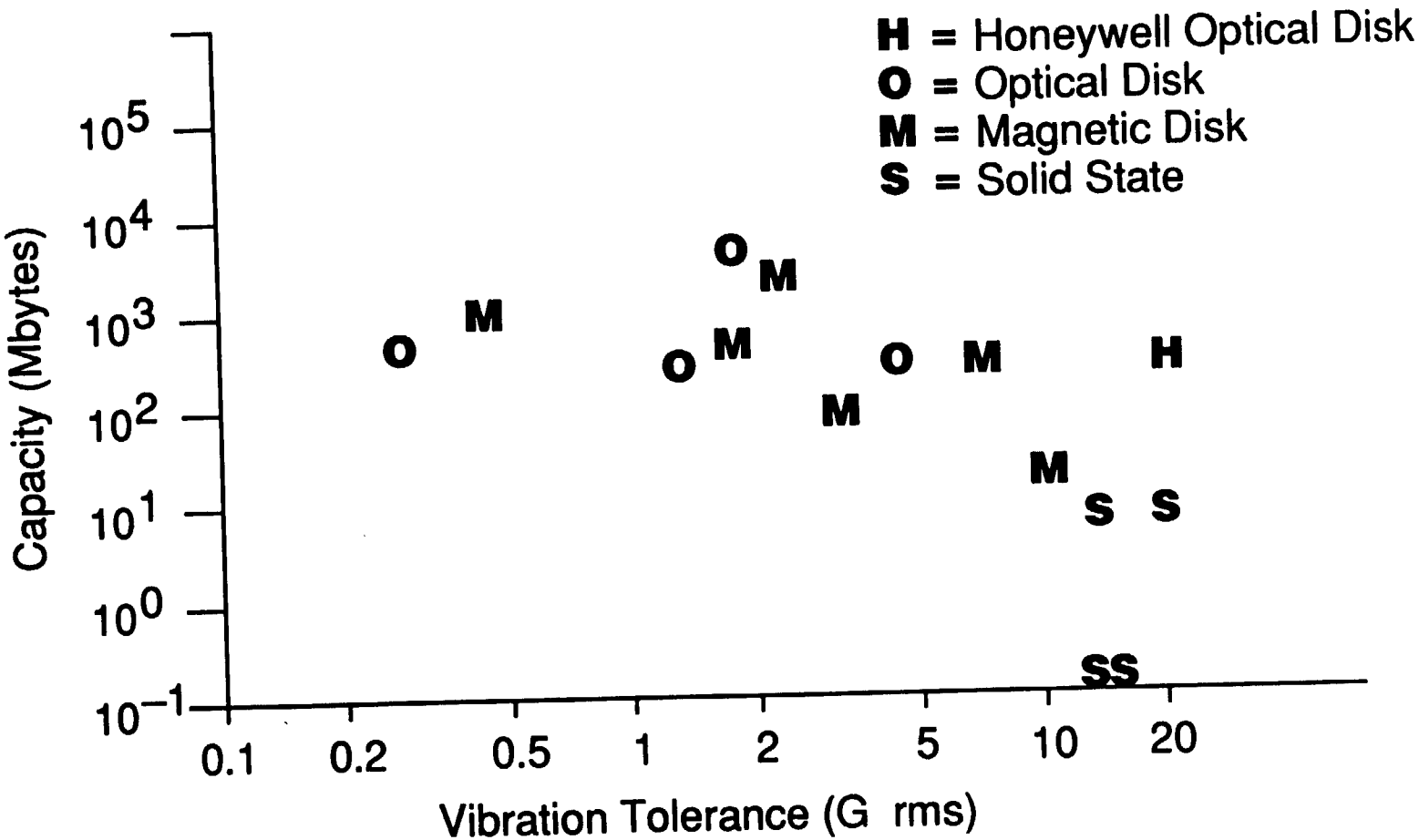
Ruggedized Memory Technologies for Aerospace Applications



**Disks on per-platter basis; electronic memories on per-box basis.*

Advanced Avionics
Johnson Space Center

Capacity vs. Vibration Tolerance of Memory Products for Aerospace Applications



Honeywell

C910778-18

Systems and Research Center

Advanced Avionics
Johnson Space Center

Environmental Performance Comparisons (Operating)

Environmental Condition	Honeywell Optical Disk Set	NASA Requirements		
		As Defined in Phase 1 Study	As Defined in Phase 2 RFP	Rockwell STS Aft Avionics Bay
Temperature	–54 to 90°C	–54 to 71°C	–48 to 35°C	–62 to 65°C
Humidity	0–100% Noncondensing	0–95%	Up to 100%	0–100%
Pressure	37–828 Torr	0–1000 Torr	672–776 Torr	0–800 Torr
Shock	15 G (11 ms)	20 G	—	20 G
Vibration	20 G rms (15–2000 Hz)	8 G rms	31.7 G rms (20–2000 Hz) worst axis	4.88 G rms (20–2000 Hz)
Salt spray	5% concentration for 96 h	—	As in coastal regions	5% concentration for 120 h
Sand and dust	MIL-STD-810D, procedure 510, method 1	—	Withstands with proper closures	Withstands with proper closures

Proposed Blue Laser Data Storage System Program

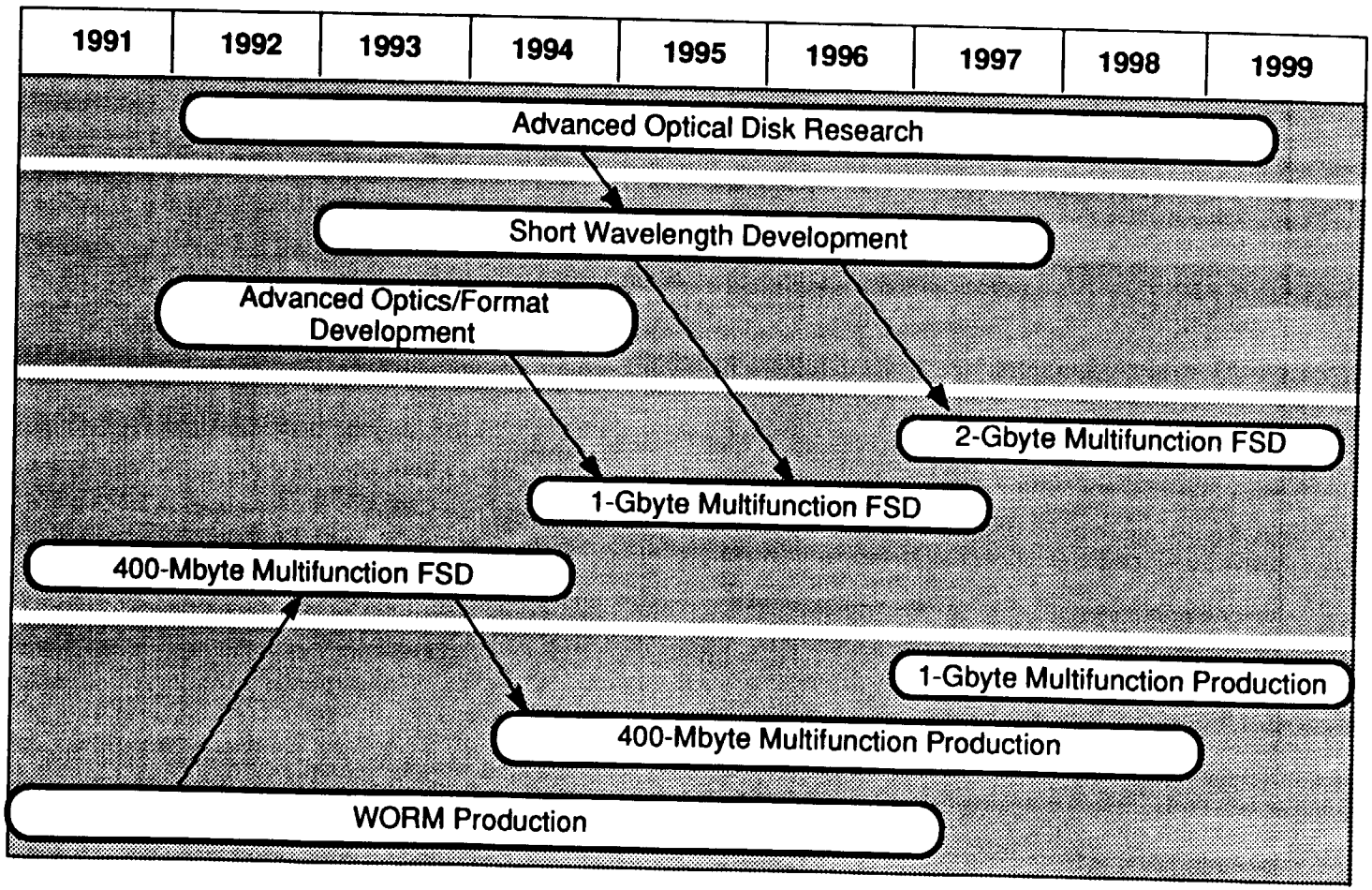
Technical Program Milestones

Optical head design incorporating blue laser source	6 months
Optical head fabricated and tested (argon laser)	18 months
Feasibility of wide gap semiconductor injection laser source	21 months
Testbed developed	30 months
Proof-of-concept demonstration complete	36 months
Development and ruggedization plan	36 months

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

Optical Disk Technology Road Map



Advanced Avionics
Johnson Space Center

Integrated INS/GPS

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

H764-C3
Inertial Navigation System with Embedded GPS

Proven Technology

Variety of applications
Inflight alignment
Hover hold
Unaffected by flight envelope or terrain
Tightly coupled mechanization
Provides optimum performance from GPS and INS
Available now

Features

- Quick reaction
- Improved location capability
- Update from overflights not required
- Precise outputs for weapons
- Jitter-free display
- Flight control outputs
- Very low life-cycle costs
- Two-level maintenance
- Heating or cooling not required
- No scheduled maintenance
- No recalibration
- No flight line test equipment
- Extensive BIT

Mean time between failure: >4000 h

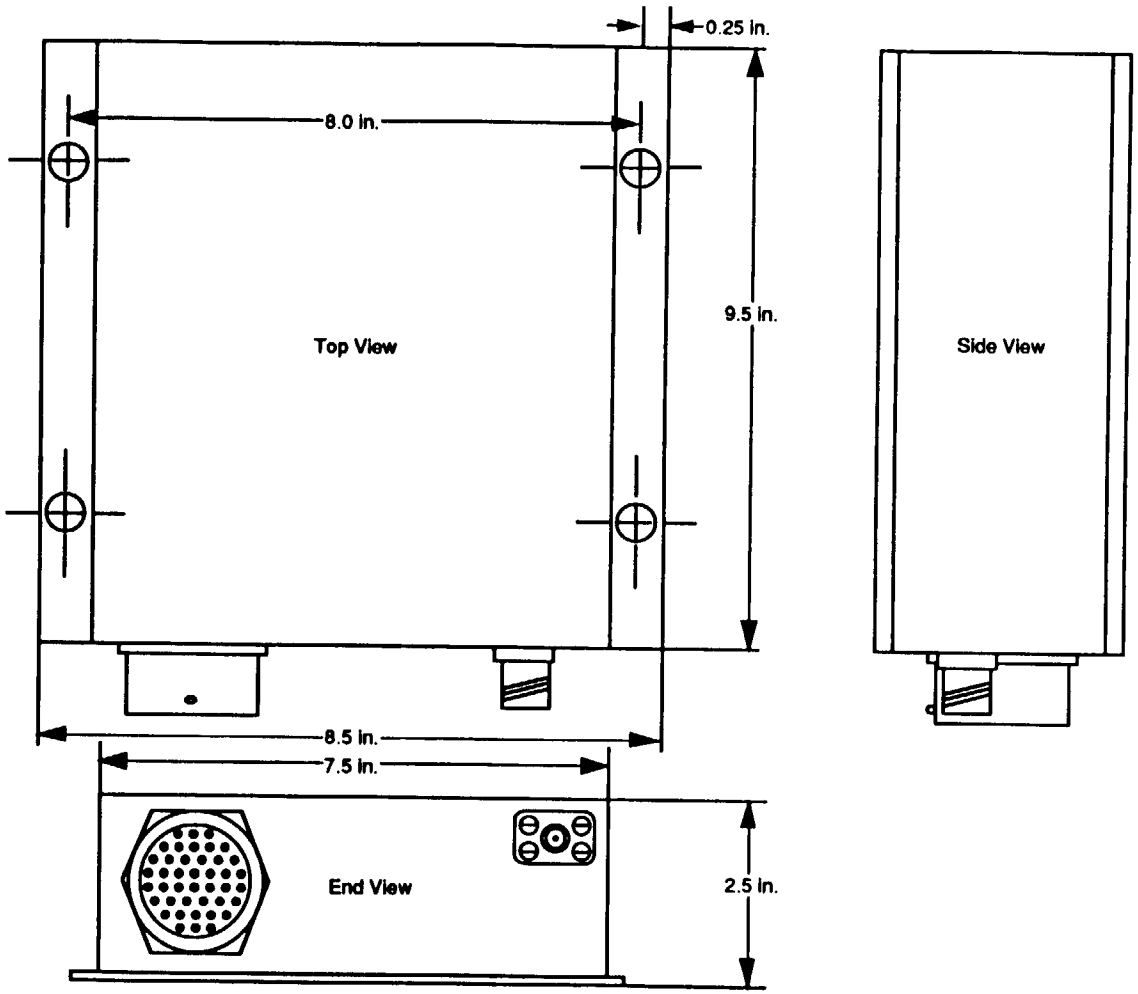
Advanced Avionics
Johnson Space Center

Other COTS Products

COTS FOR SPACE

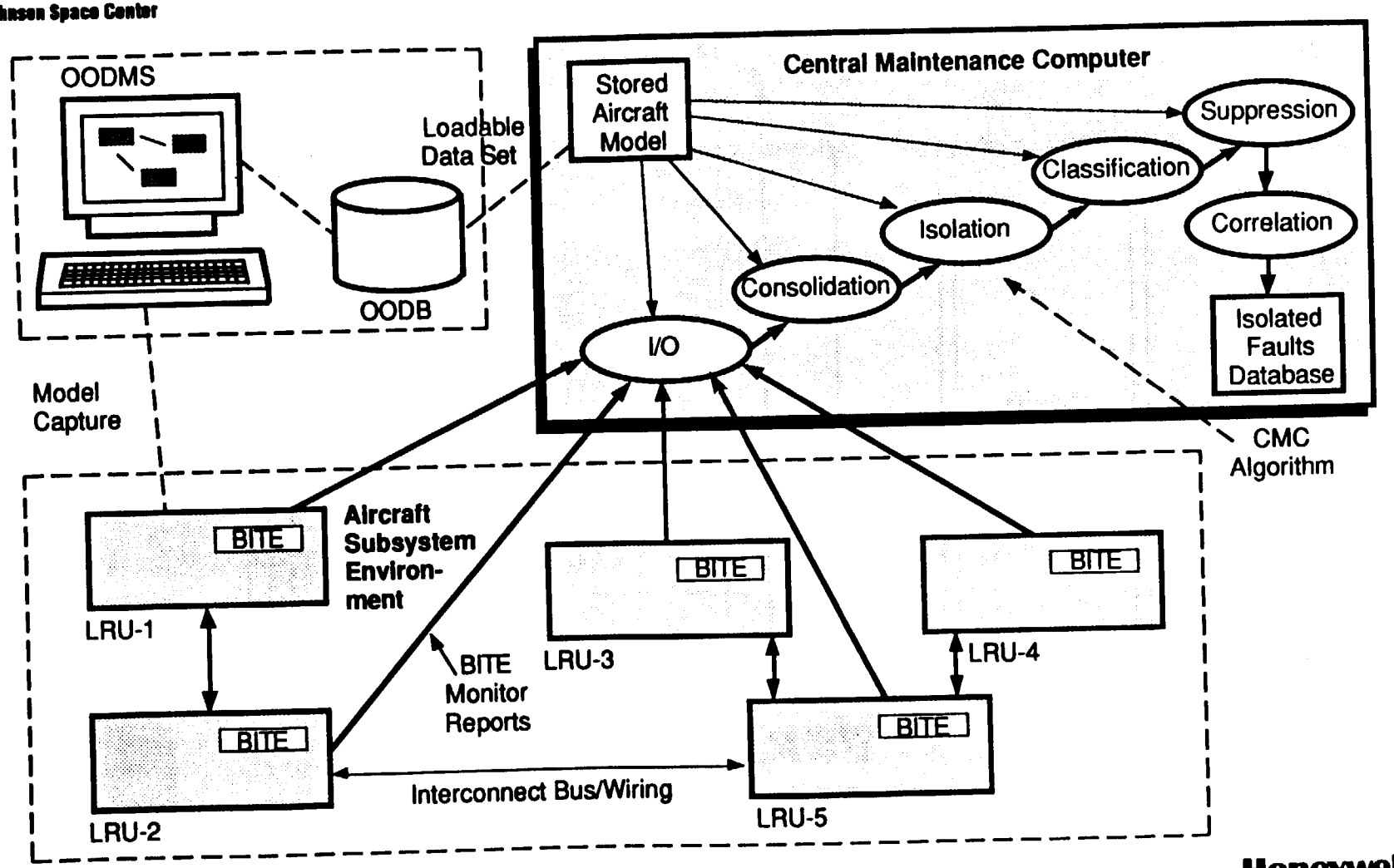
Advanced Avionics
Johnson Space Center

GPS/Glonass Sensor Unit
ARINC 743A



Central Maintenance System Concept

Advanced Avionics
Johnson Space Center

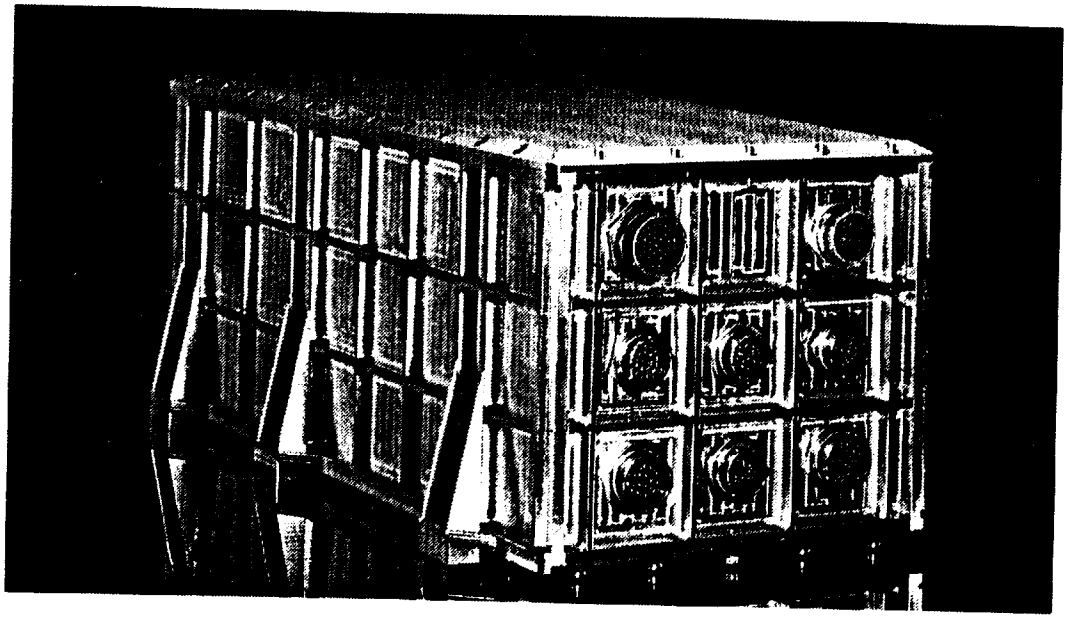


Honeywell

Honeywell

HEXAD

6 Sensor / Dual Fault-Tolerant Inertial Navigation System



Specifications

Volume	1615 in^3
Weight	<60
Power	<150W
Temperature Range	-30° F to +145°F
Vibration	23 grms
Shock	2000 G
Gyros	(6) GG1320
Accelerometers	(6) QA3000

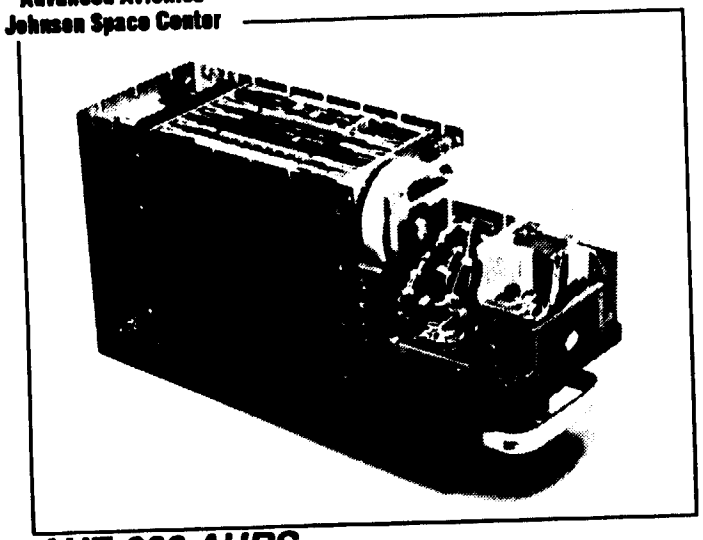
Features

- Unmatched mission success (greater than 0.9999)
- One unit replaces three
  - — Low weight, power, size and cost
- MIL-STD-1553B Interface
- No customer calibration
- 30% better accuracy (0.707 better than Triad)
- Fail-op, fail-op, fail-safe

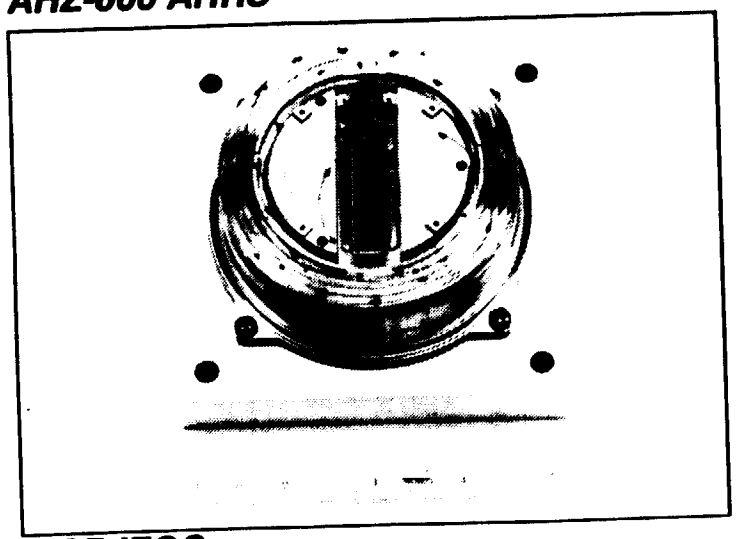
Fiber-Optic Gyros (FOGs)

COTS FOR SPACE

Advanced Avionics
Johnson Space Center



AHZ-800 AHRS



GGP IFOG

Honeywell—the leader in optical gyro technology

- IFOG and RFOG
- First IFOG products
  - AHZ-800 AHRS
  - Boeing 777 SAARU
- GGP-integrated nav system
  - Nav-grade IFOG
  - Tightly coupled GPS system
- Tactical grade IFOG
- Satellite IFOG
- Nav-grade RFOG

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

F-16 Flight Control Maintenance Diagnostic System

Type—AFFDL contract ($4.0M)

Goal—show improved fault diagnosis through RTOK/CND reductions and flight line presentation of technical information

Approach

- Model-based reasoning guides troubleshooting
- Model covers functional structure, tests, and aircraft state
- Test selection and prioritization

Milestones

6/85	Contract start
4/89	MacDill AFB system evaluation
12/89	System hosted on Agilis (hand held) computer

Plans

- Field tests at Luke (9 months) and Hill (6 months) AFBs using an AF dedicated F-16
- Incorporated suggestions from AF in Block 40 aircraft

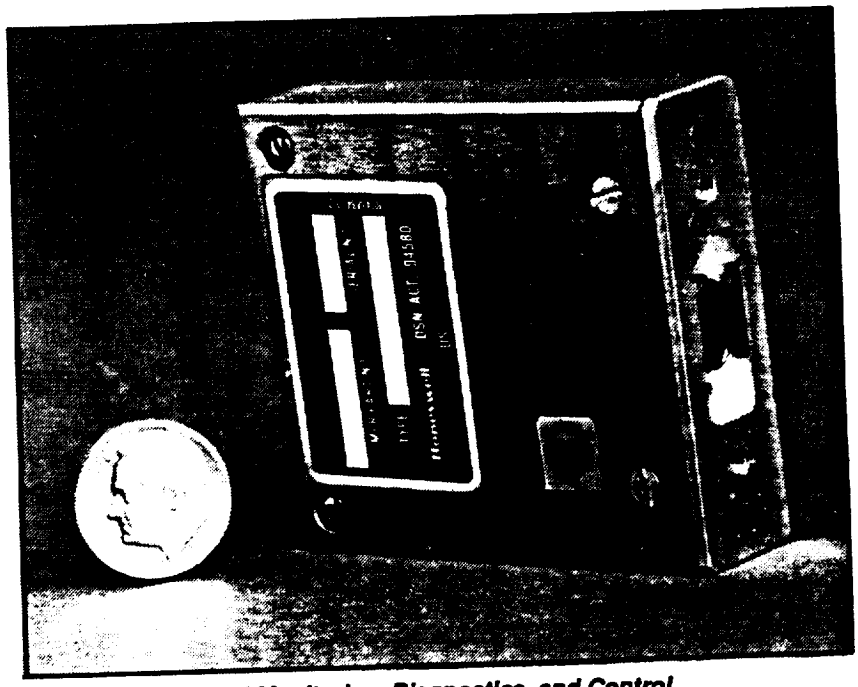
HG-1128AA01 Smart Instrumentation Module System (SIMS)

Advance Information

Description

The HG-1128AA01 Smart Instrumentation Module System (SIMS) is a universal sensor interface that integrates low-power sensor preprocessing electronics with application-specific sensors to provide embedded sensing and monitoring for health management applications and sensing and actuation for control applications. It is designed to increase system availability and lower-life-cycle cost by reducing both the time required for inspection and the need for scheduled maintenance.

The SIMS is programmable to receive input from a variety of sensors or to accommodate different sensor parameters. System capabilities include data logging, local qualification and decision making, self-calibration, fault and anomaly detection, diagnostics, and embedded control.



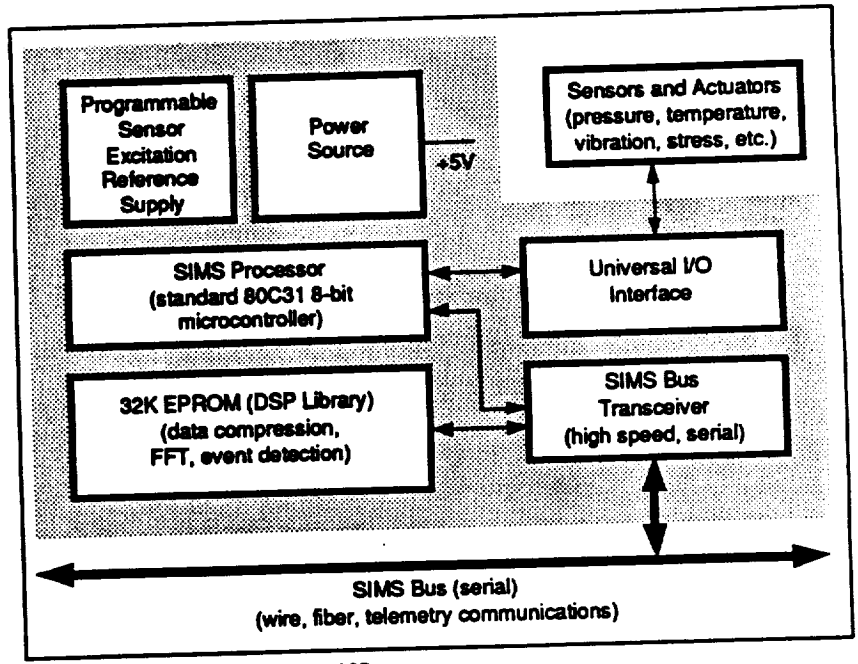
SIMS for Embedded Monitoring, Diagnostics, and Control

Features

- Universal sensor (I/O)
- Small package
- Low power
- Extensive digital signal processor (DSP) algorithm support
- Flexible bus (I/O)
- Multiple high-resolution analog-to-digital converters
- Military qualified

Applications

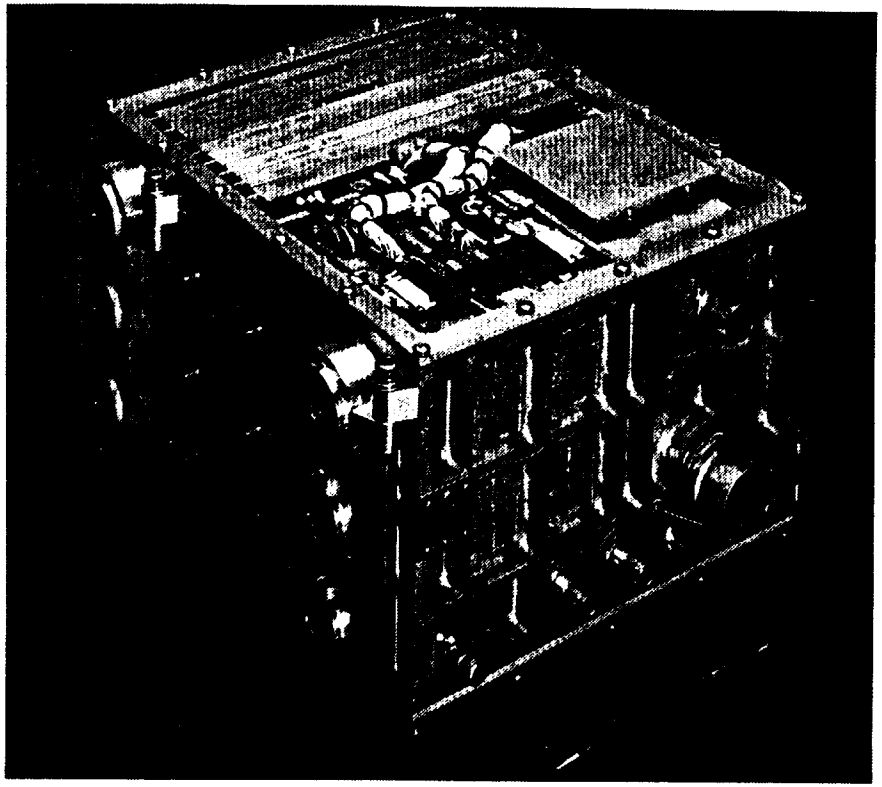
- Avionic system diagnostics
- Aerospace system environmental monitoring
- Air data/flight control system monitoring
- Local-loop industrial control
- Test data acquisition



Functional Schematic of SIMS

Inertial Measurement Unit

GG1320
Ring Laser Gyro



Specifications

Size:	10.25x08.5x06.5 in
Weight:	28 lb
Power:	70 W at 28V dc
Operating Temp:	45° to +110°F
Vibration:	21 grms
Gyros:	GG1320
Accelerometers:	Bell XI-82

Features

- **10 X the accuracy of small navigation units**
- **No prelaunch calibration or alignment required**
- **Circumvention and recovery built into the hardware and embedded in software**
- **Improved life, MTBF**
- **R&D activity in progress to reduce size to 277 in^3 and 11 lb**

Advanced Avionics Software Issues

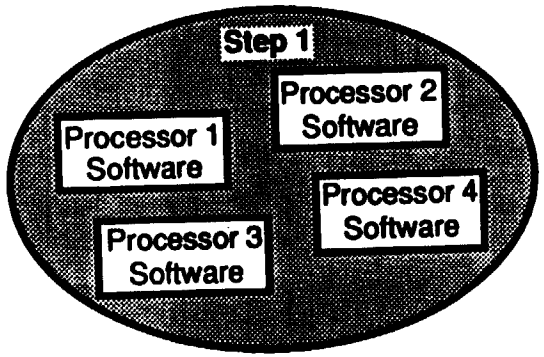
Advanced Avionics
Johnson Space Center

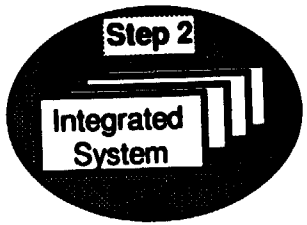
Creating reliable distributed software is one of the major problems facing modern avionics system developers

Conventional Method

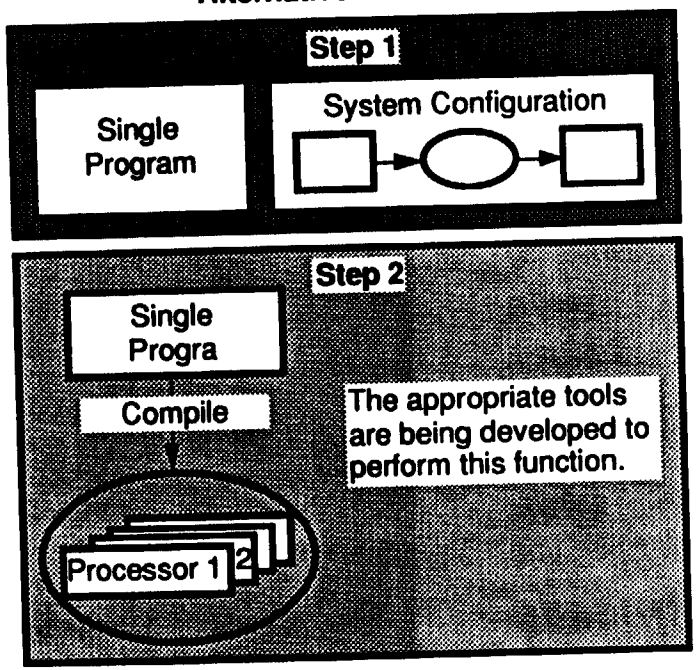
Some examples of potential problems

- Compiler cannot check compatibility of data types between various fragments
- Name binding, scoping, context usage, timing, etc.
- Proof of correctness





Alternative Method



Honeywell

Systems and Research Center

Appendix B
Supporting Viewgraphs and Annotations

Contents

Advanced Avionics
Johnson Space Center

Introduction

- Purpose, goals, objectives, and benefits
- Definitions
- Approach

Advanced Avionics
Johnson Space Center

Purpose, Goals, Objectives, and Benefits

Advanced Avionics
Johnson Space Center

Commercial Applications in Space

Commercial avionics and avionic requirements/procedures are highly applicable to space avionic systems.

Advanced Avionics
Johnson Space Center

Study Goal

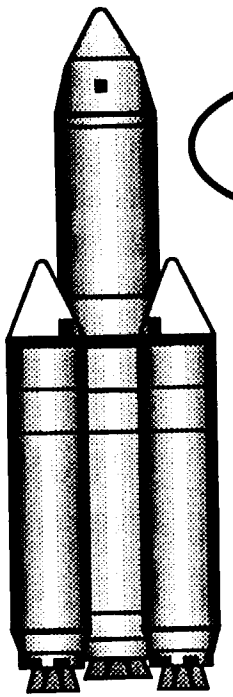
Test the integration of commercial-off-the-shelf components, products, and technologies in space applications

MD 11

Airbus

Boeing 777

Application



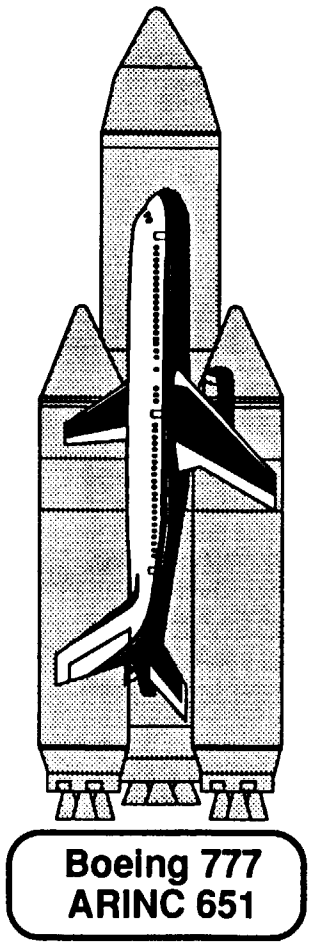
SEI

EDO

NLS

Advanced Avionics
Johnson Space Center

Study Objectives



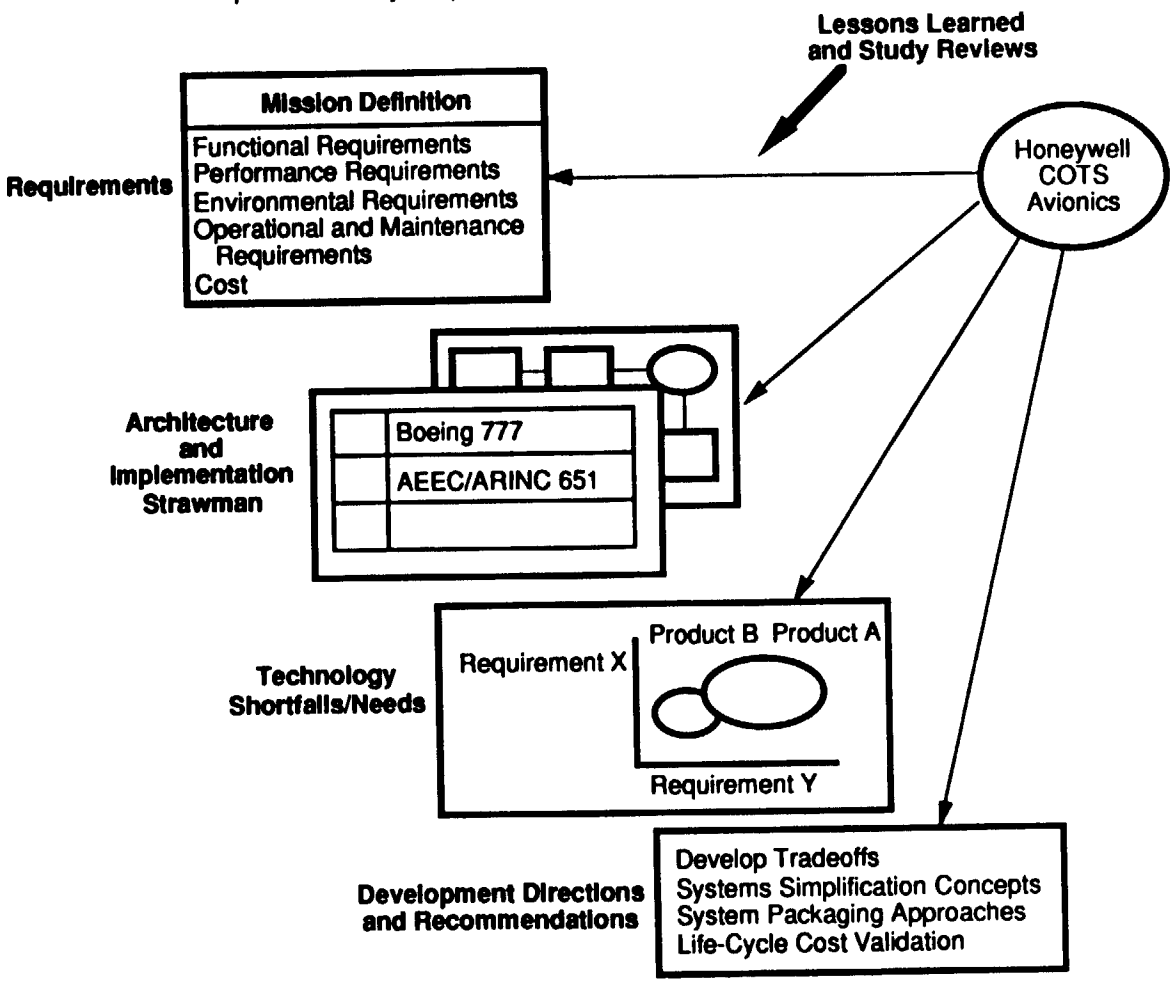
Will commercial avionics do the job?

Improvements needed?

Advanced Avionics
Johnson Space Center

Program Objectives

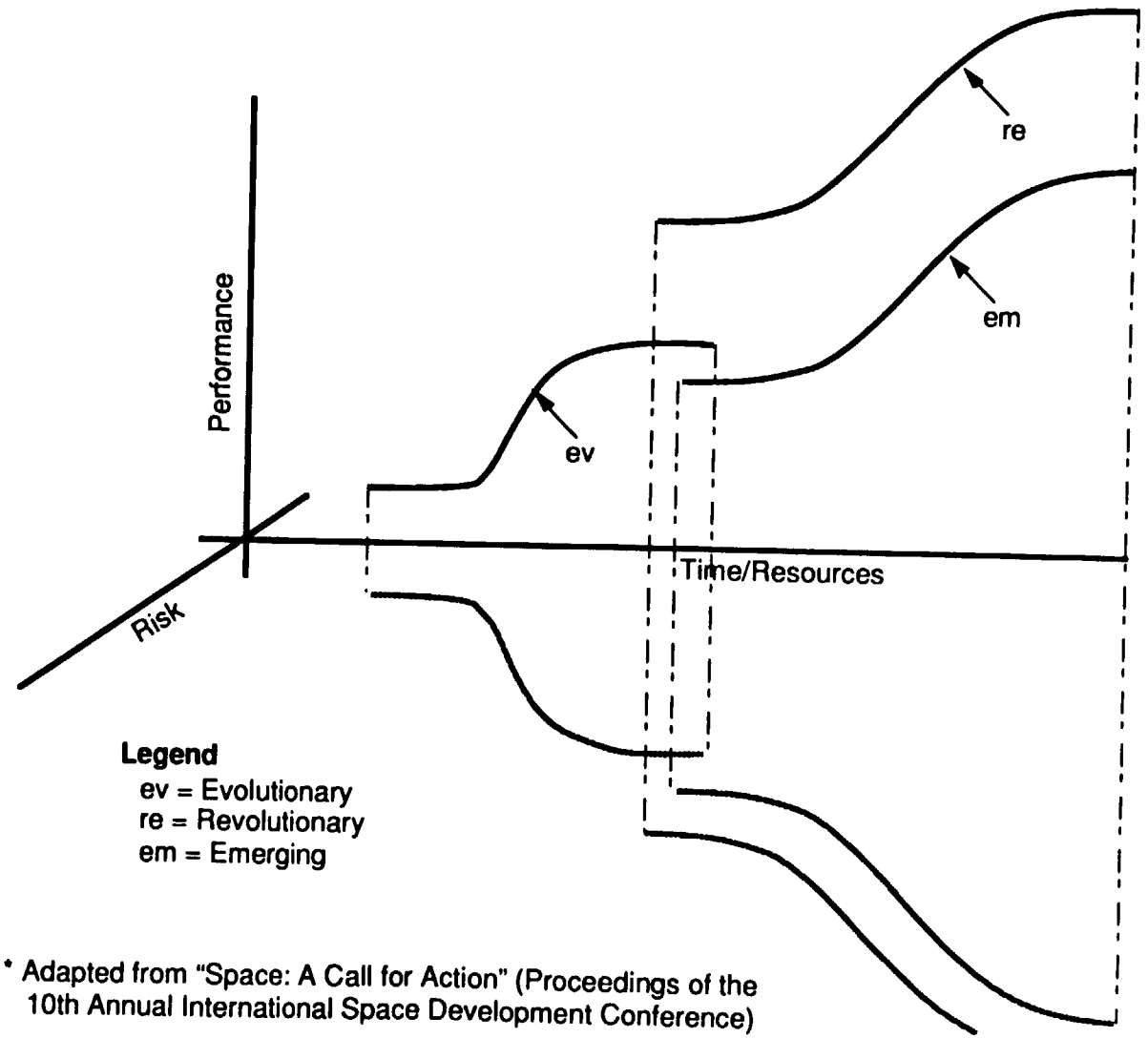
- Greatly improve national launch capability
- Reduce operating costs
- Improve reliability, responsiveness, and mission performance



Honeywell

Advanced Avionics
Johnson Space Center

Possible Technology Performance*



Legend
ev = Evolutionary
re = Revolutionary
em = Emerging

* Adapted from "Space: A Call for Action" (Proceedings of the 10th Annual International Space Development Conference)

Advanced Avionics
Johnson Space Center

Commercial Avionics Experience*

- Aircraft maintenance programs are developed to take advantage of extensive onboard test and diagnostic capabilities.
- Future commercial aircraft will have sophisticated integrated functional test systems.
- Incremental improvements in flight hardware are approached through integration.
- Commercial airlines often make decisions based on experience and history (very large number of flights). A key phrase often used is "Experience has shown. . .". This is not the case for all expendable vehicles.

* M. Raftery, Boeing, "The Application of Commercial Airplane Avionics to Advanced Space Transportation," AIAA 90.

Advanced Avionics
Johnson Space Center

Commercial Avionics Requirements

Commercial avionics (AIMS) requirements are highly applicable to future space-based avionic systems:

- Lower life-cycle costs
  - Elimination of I/O and power supply duplication
  - Reduced spares cost; spares are modules, not today's LRUs
- Reduced weight, power, wiring, and volume
- Greater flexibility for future growth
  - Take advantage of new technology without architectural changes
  - Accommodate system upgrades without hardware changes
- Commercial bus development requirements
  - Robust partitioning; no failure propagation
  - Reliability; aggressive no-maintenance policy
  - Fault tolerance; no single failure can cause loss of essential avionic functions
  - Flexibility; support many module types; must allow addition/modification of new functions
  - Easy to debug and certify; predictable
- Software partitioning requirements
  - No two partitions can have access to the same memory location
  - The failure of one partition cannot cause another partition to fail, nor can it prevent another partition from resource access
  - Presence of other partitions should be invisible (virtual machine)

Advanced Avionics
Johnson Space Center

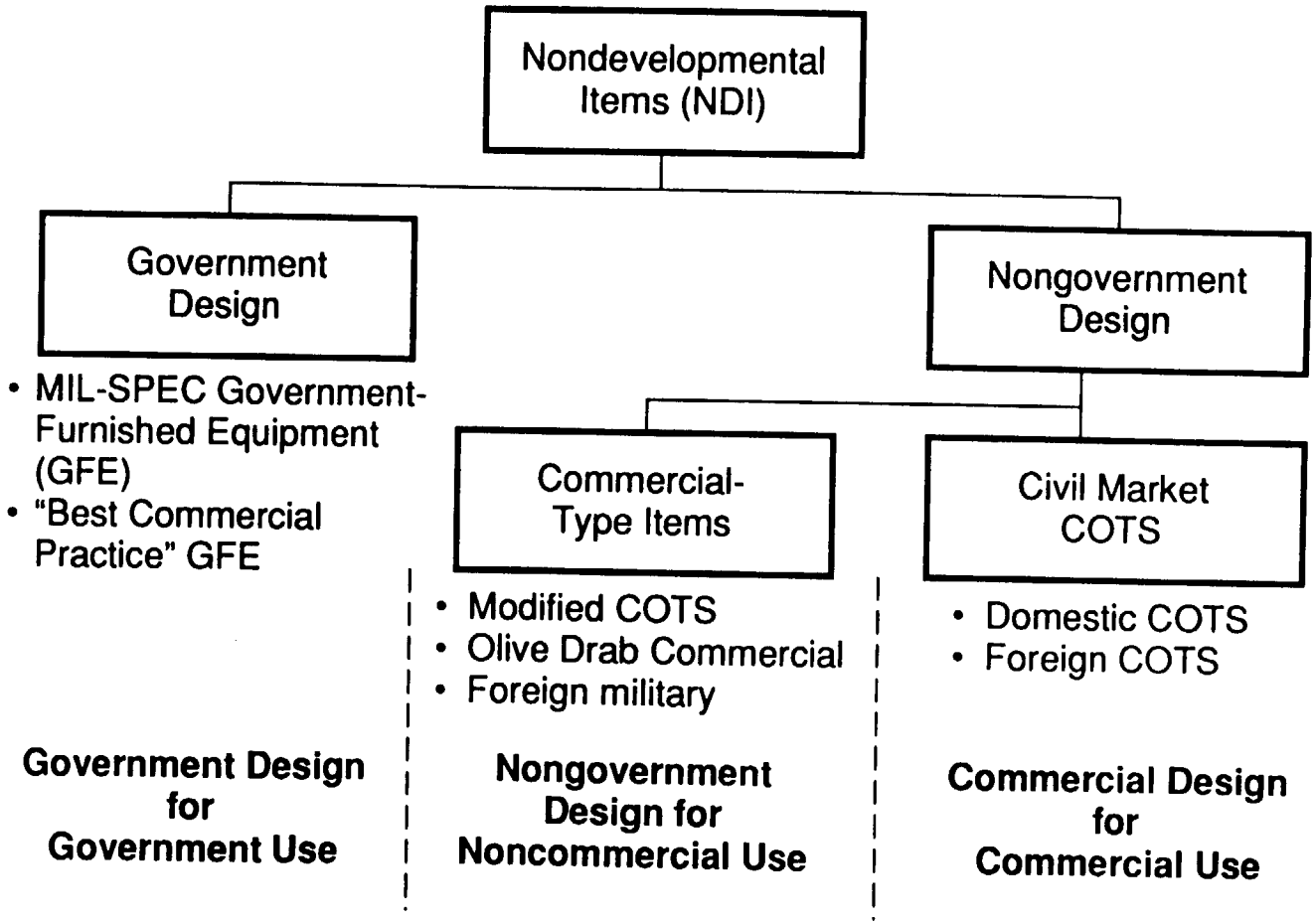
B-14

Definitions

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

Nondevelopmental Items



Reference [USAF22]

Advanced Avionics
Johnson Space Center

The Commercial Spectrum

	MIL-SPEC	Best Commercial Practice	Olive Drab Commercial	Commercial-Type ("Special")	Civil Market COTS
Design Features	Government: militarized	Government: not militarized	Commercial: just for government	COTS: modified for government	For civil market
Examples	Fighter aircraft	Fixed ground radio	Tactical radio	Embedded computer	Television monitor
Percent of Sales to Government	100%	100%	Probably 100%	Small (of basic item)	Small
Design Disclosure	Full (piece part)	Full (piece part)	Mostly F3* May be full	Probably F3* Full needed	F3*
Configuration Authority	Government	Government	Vendor or foreign government	Domestic or O/S vendor	Domestic or O/S vendor
Design Stability Risk	Low	Low	Moderate to low	Moderate to high	High
Long-Term Support/ Cost Risk	Low	Low	Moderate	High	Moderate to high

*Form, fit and function

Reference [USAF22]

Advanced Avionics
Johnson Space Center

Approach

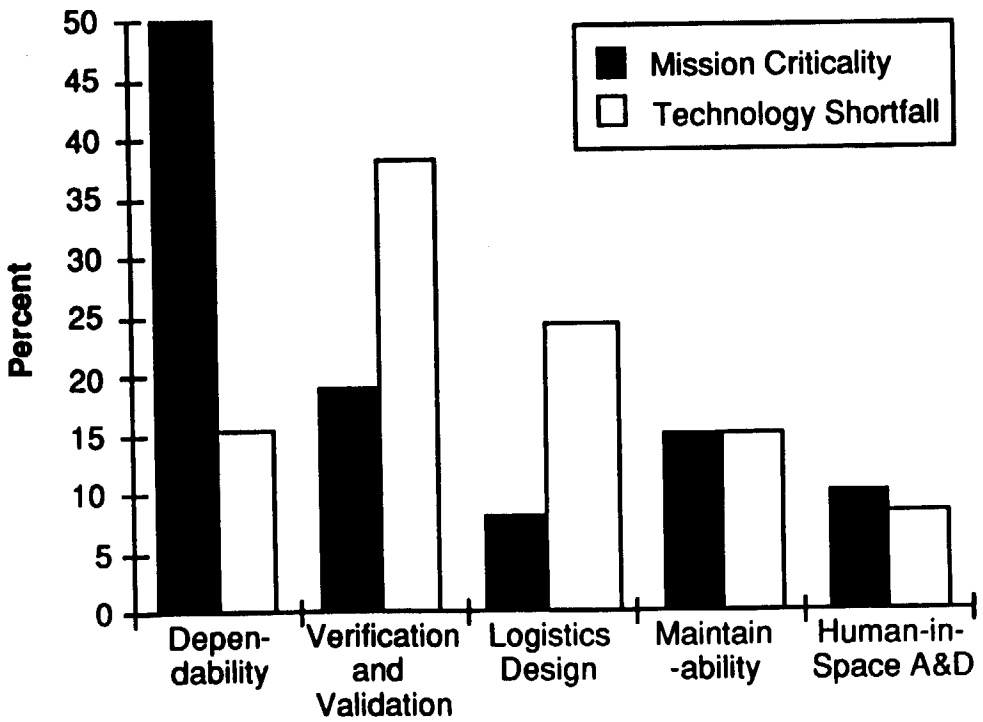
Advanced Avionics
Johnson Space Center

Technology Assessment Approach

- Results should consider both program requirements and technology capabilities
- Saaty reanalysis (chart follows)
  - Categories: systems design, hardware, software
  - Importance: mission criticality and technology shortfall

Advanced Avionics
Johnson Space Center

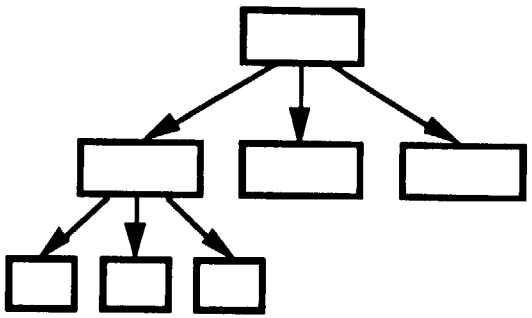
Systems Design Concerns



Advanced Avionics
Johnson Space Center

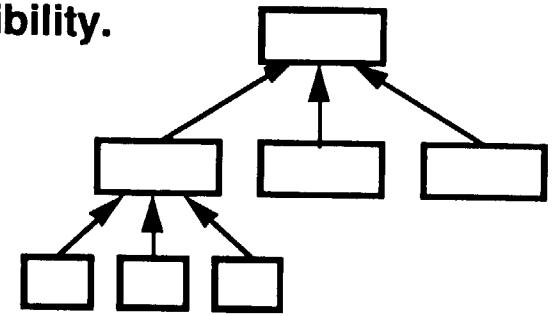
Advanced Avionics Requirements Development Issues

With a top-down approach we can miss some very important real-world issues.



Example: Weight minimization goals and availability of software preclude use of hardware FDIR. Failure response timelines, software reliability, and V&V costs are not considered.

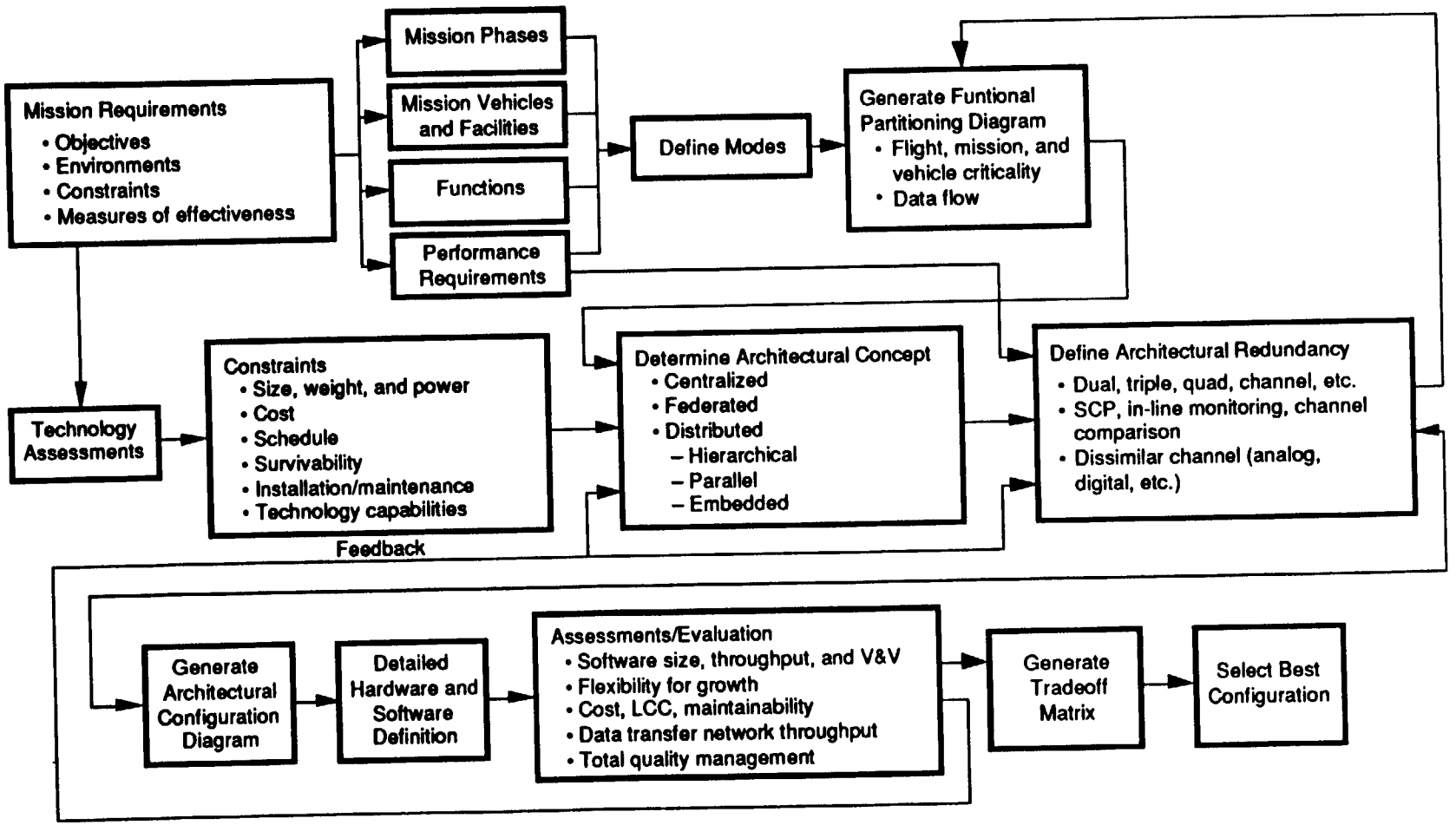
With a bottom-up approach we sometimes do not address implementation feasibility.



Example: Low-radiation-tolerant parts at the module level require extensive avionics bay shielding.

A combination top-down, bottom-up "self-checking architectural design process" is used to assure COTS study consistency

A Self-Checking Architectural Design Process



Advanced Avionics
Johnson Space Center

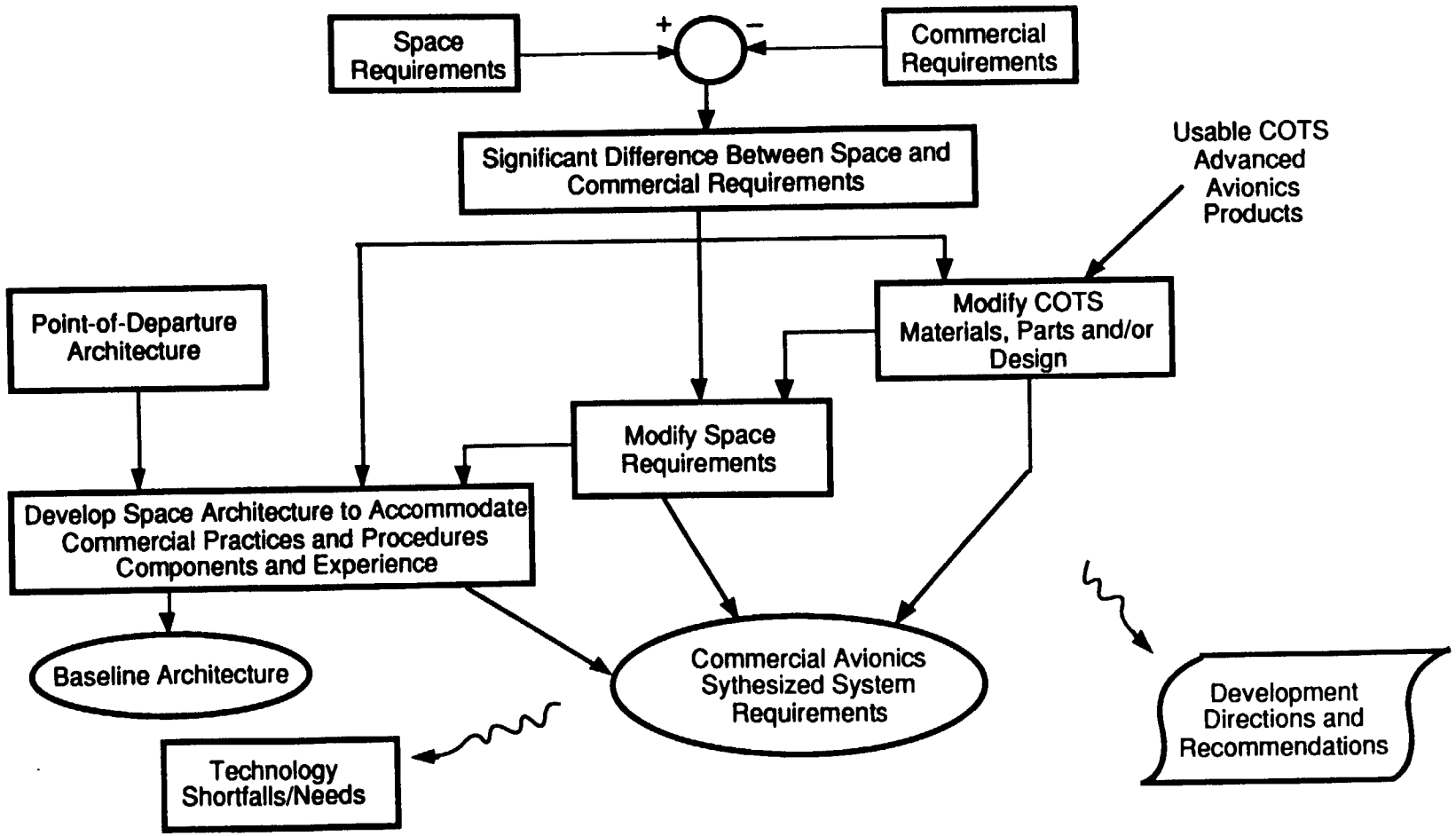
Architecture Requirements Comparison

Requirements	Advanced Avionics System Requirements	Nondevelopmental Item Design Requirements	
		Military	Commercial
Cost	Low	High	Low
Reliability	High	High	High
Maintainability	Space	Ground/war	Ground
Useful Life	90 days/20 years	20 years	20 years
Safety	High	High	High
Quality Assurance	High	High	High
Transportability	High	High	High
Health Monitoring	High	Medium	Medium
Commonality	High	High	High
Environmental			
• Acceleration	ETO	Maneuvers	Low
• Vibration	ETO	High	Low
• Shock	Docking/landing/ETO	Hits	Landing
• Electromagnetic	Space	Electronics	Electronics
• Thermal	2800W/m^2	Medium	Medium
• Contamination (dust)	High	Medium	Low
• Meteorite	Yes	No	No
• Radiation	GCR/SPE	No	No
• Partial vacuum	Yes	Some	No
Performance	High	High	High
Physical			
• Size	Small	Small	Small
• Mass	Light	Light	Light
• Power	Low	Low	Low
Materials	Outgassing	Minimum	Minimum
Autonomy	High	Medium	Low
Reusable/Expendable	Both	Reusable	Reusable
Manned/Man-Rated/Unmanned	Man-rated	Manned	Manned
Growth/Flexibility	High	Medium	Medium

Shaded areas indicate significant differences between commercial requirements and space requirements of this study

Advanced Avionics
Johnson Space Center

Advanced Avionics Synthesized Requirements



Advanced Avionics
Johnson Space Center

Typical Modifications Required to Space-Qualify Optical Disk Drives

- Mechanically redesign to survive space environment
  - Optical disk media
  - Disk drive
  - Optical read/write head
  - Motors and actuators
  - Electronics
  - Packaging
  - Thermal design

- Electronically redesign to survive space and environmental parts requirements
  - Circuit components
  - Circuit modularization and card layout
  - Connectors

- Built-in test/maintenance design to meet space requirements

Advanced Avionics
Johnson Space Center

Architectural Approach

- Flexible integration—from transitional COTS+ integration to COTS+ framework with a minority of space-qualified products

- Universal applications
  - All future manned/unmanned space missions/vehicles
  - Backward integration
  - Surface applications

- Universal architecture
  - Standard interfaces (multistandard)
  - Open architecture
  - Modular avionics
  - ARINC 651*
  - LRU subsystems compatible

- Cost-effective

* Special acknowledgment and appreciation is given to the AEEC for permission to incorporate ARINC 651 concepts into this study.

Advanced Avionics
Johnson Space Center

Modular Avionics

Modules That Perform Basic Electronic Functions

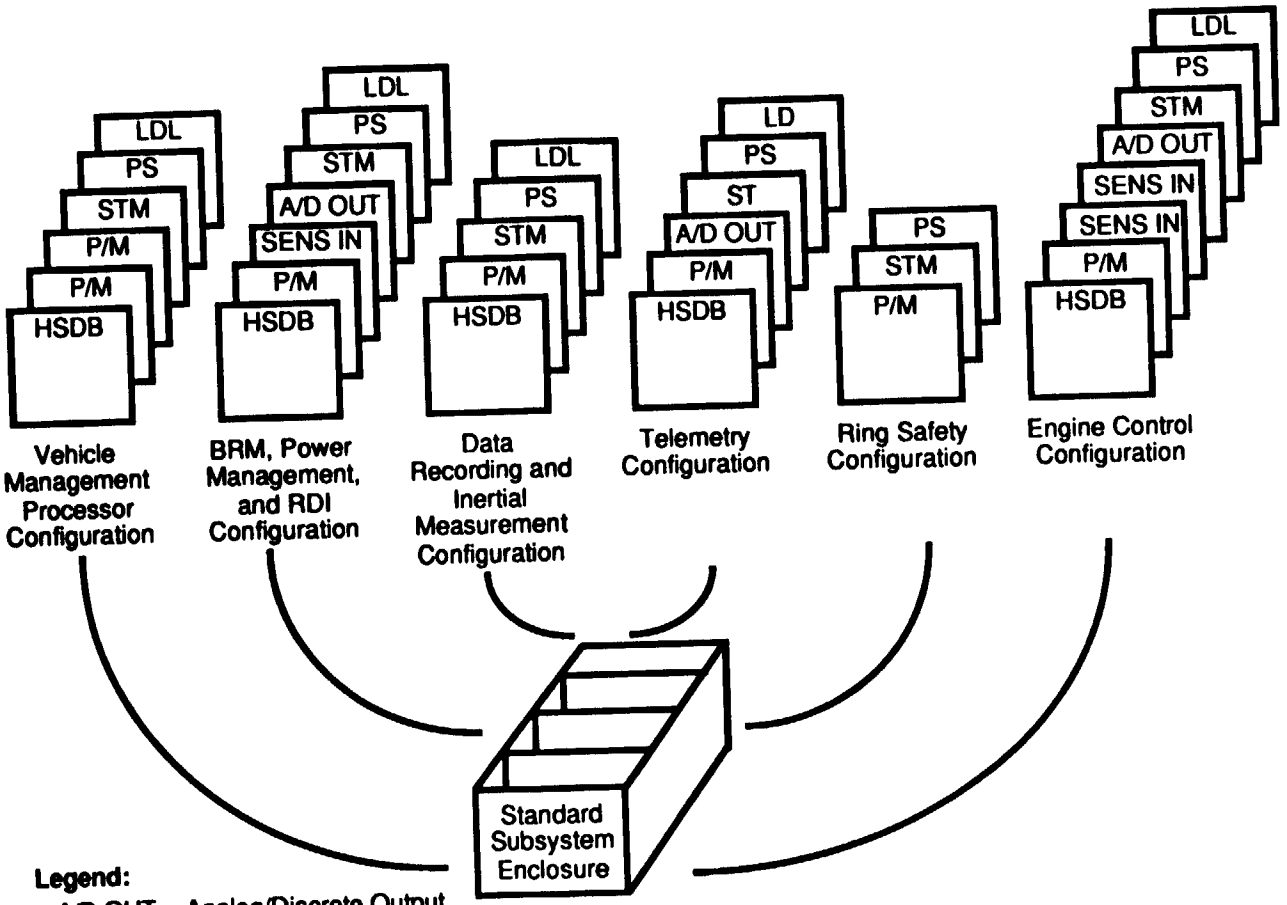
- Processor/memory
- System network interface
- Local data link
- Sensor input
- Analog/discrete output
- System test and maintenance
- Power supply

Advantages of MS*

- Standardization of mechanical and electrical interfaces
- Use of common hardware and software modules
- Shared development costs
- Larger production runs
- Shared support facilities and spares
- Increased competition for components
- Streamlined maintenance support requirements
- Support for integrated system designs
- Enhanced adaptability and expandability
- Simplified future upgrades
- Simplified new technology introduction
- Effective implementation of fault tolerance through redundancy and reconfiguration
  - Improved availability
  - Improved mission reliability
  - Reduced demand for line maintenance

* Source: *Modular Avionic Handbook*, 18 April 1990, Modular Avionics Systems Architecture (MASA), United States Air Force, Wright-Patterson Air Force Base.

Modular Packaging



Legend:

A/D OUT = Analog/Discrete Output
HSDB = High-Speed Data Bus
LDL = Local Data Link
P/M = Processor/Memory
PS = Power Supply
SENS IN = Sensor Input
STM = Standard Test and Maintenance

Source: MPRAS GD Report

Advanced Avionics
Johnson Space Center

Lessons Learned

- Study reviews
- Reference inputs
- Lesson learned

Advanced Avionics
Johnson Space Center

Lessons Learned and Study Reviews

The following sheets provide examples of lessons learned and documented within this study. The lessons are derived from space programs and space study reviews. The lessons learned, once justified, are incorporated within the System Requirements Specifications.

Justification of requirements must be provided by the source or developed herein; otherwise the requirements will not be used. Studies are critiqued as part of this study.

Advanced Avionics
Johnson Space Center

Extended-Duration Orbiter Avionics Requirements

Functional Requirements—The avionics system will perform the following functions:

- Major Mode 305 Automation—The EDO avionics system will have a backup mode that will provide automatic control of the orbiter GN&C during the terminal area energy management (TAEM) and approach/landing phases. This portion of the entry flight profile encompasses major mode 305 with the following two phases:
  - TAEM (305)—This phase of major mode 305 contains all functions necessary to monitor, guide, and control the vehicle from initiation of the TAEM phase to the autoland interface. TAEM will be exited by an automatic transition to the approach/landing phase.
  - Approach/Landing (305)—This phase of major mode 305 contains all the functions necessary to monitor, guide, and control the vehicle from initiation of the approach/landing phase to nosewheel touchdown.

- WOW Redundant Sensors—The EDO Orbiter Avionics System will have redundant weight on wheels (WOW) sensors to provide for automatic main landing gear wheel touchdown confirmation. The WOW sensing shall be doubly fault tolerant.

Advanced Avionics
Johnson Space Center

Extended-Duration Orbiter Avionics Requirements (continued)

Performance Requirements—The EDO orbiter avionics system performance will be defined as follows:

- Autoland—The EDO orbiter avionics will have the capability to perform autoland in major mode 305.

- Approach/Terminal Area Energy Management—The GN&C from post-blackout until landing glide slope and NAVAIDs have been acquired shall perform the functions as specified in paragraph 3.3.5.1.8 of the Orbiter Vehicle End Item (OVEI) specification.

- Landing and Rollout—The EDO orbiter GN&C in conjunction with associated subsystems shall provide for orbiter automatic landing (following acquisition of terminal area RF landing aid signals) through nosewheel touchdown.
  - Transition from the final approach flight path will be accomplished such that the rate of change of flight path is less than 0.5 deg/s for a period not less than 5 sec prior to final flare. Normal acceleration load during the transition maneuvers shall not exceed 0.5 g nominal value.

Advanced Avionics
Johnson Space Center

Extended-Duration Orbiter Avionics Requirements (continued)

- Touchdown conditions shall be compatible with a safe landing on a 15,000-ft x 300-ft lakebed runway with wind conditions as specified in OVEI Appendix 10.1.

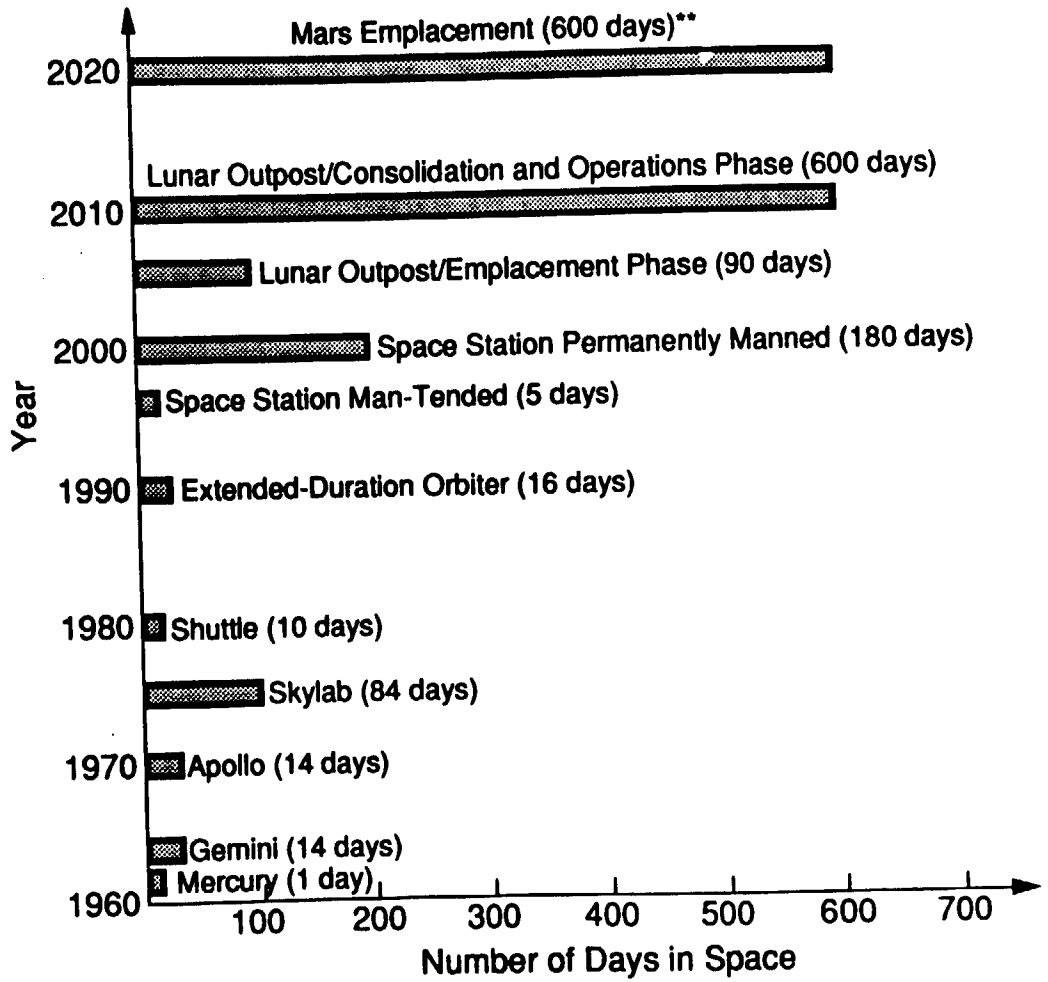
- The GN&C, with landing and RF navigation aids, shall control the orbiter during approach and landing within the following limits:
  -- Crab angle shall be maintained at less than ±10
  -- Lateral displacement from the runway centerline at pre-flare shall be less that ±50 ft

- Touchdown conditions to be achieved (reference and tolerances) are based on flight performance and orbiter limits as specified in the applicable paragraphs of the OVEI specification. Constraints to landing performance/conditions include runway width and length, tailscrape, landing gear, loads, and structural limitations. Representative values for satisfying landing performance constraints are provided in Table 3.2.8.2.2.1.1.2-1, governing specifications requirements.

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

History of Human Space Flight Life Span*



* Times are mission elapsed per crew.

**Option 5, 90-day study.

Source {Krishen]

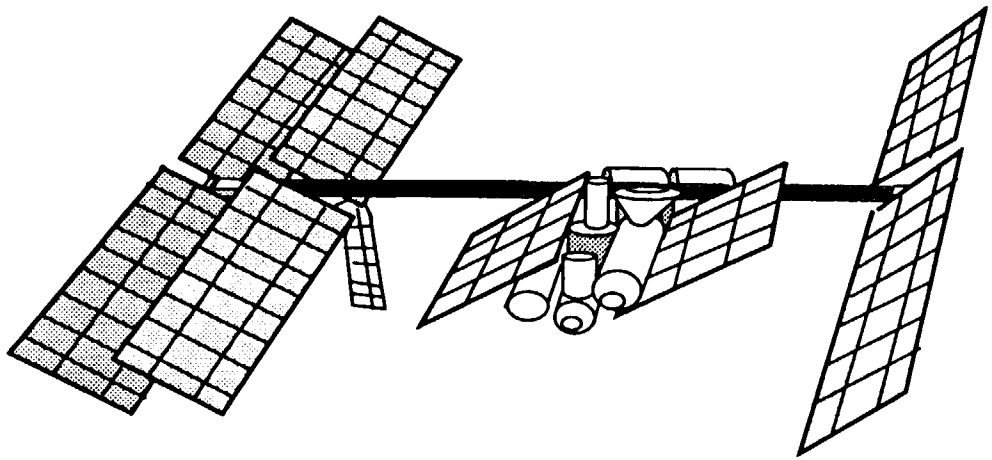
Honeywell

Systems and Research Center

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

Space Station Freedom



- Provides permanently manned international facility
- Provides three fully equipped microgravity labs
- Focuses on microgravity and life sciences
- Provides exposed facility for external payloads
- Provides ample power

Advanced Avionics
Johnson Space Center

Boeing's Reliability Study Summary*

- Even if ultra-reliable electronics components are available, single-string systems are not an option, except for the "shortest" missions
- For ETO missions, dedicated and pooled sparing appear to be viable
- Longer duration missions (TEV and OSS) pooled sparing redundancy using multipurpose electronics modules will be required

*Boeing's report on "NASA Standard Avionics Requirements"

Advanced Avionics
Johnson Space Center

Summary of Lessons Learned That Have Value to Lunar Exploration Scenarios*

- Automation and robotics must be exploited to their maximum extent, including automated hardware operations and test sequences, automated fault detection and isolation, AI techniques for trend analysis and corrective action
- The design of hardware, software, and support equipment must be assessed for overall life cycle
- Assembly operations cost must be minimized by designing simple components
- Thorough ground test and evaluation programs must be used to ensure the availability of mature hardware and validated procedures
- Interfaces between flight hardware elements and surface support equipment must be minimized and simplified (interfaces between shuttle and payloads have been criticized for their complexity)
- Maintainability and operability must be emphasized throughout the program (they are often abandoned due to budget limitations)
- An effective configuration management system that does not consume significant extraterrestrial resources must be designed
- Common assemblies, systems components, and attach hardware, off-the-shelf parts, and standarized practices should be used for flight and nonflight systems
- Adequate access to hardware interfaces, attachments, and test points must be provided

*"Lunar Transportation Facilities and Operations Study," McDonnell Douglas

Advanced Avionics
Johnson Space Center

Summary of GD Space Avionics Study

- Strengths
  - Compiles a large amount of existing work
  - Reasonable taxonomy of space exploration modules

- Areas for further analysis
  - Linking of avionic requirements to mission/system requirements
  - Systems engineering approach in requirements analysis and flowdown (and up)
  - Technology shortfalls and needs vs. just shortfalls

- Recommendations
  - Provide or develop mission scenario details adequate to derive requirements
  - Use requirements for functional designs
  - Analyze candidate technologies to determine a system design that meets the requirements of the functional design

Advanced Avionics
Johnson Space Center

NLS Vehicle Flight Avionics—Modular Avionics Assessment

Preliminary Requirements	Tradeoffs	Comments
1.1 Common/portable avionics kit (CPAK) on SC, CTV, US; CPAK is controlling avionics for all flight phases	1.1 Core stage has own controlling avionics even when CTV/KS or US are flown	1.1 Issues: centralized architecture—single point of failure, availability of system
1.2 Dedicated avionics provided on core stage, CTV, and US to augment CPAK	1.2 Dedicated vs. embedded	1.2 System modularity at flight control system level, not vehicle level; what does term "dedicated avionics" mean?
1.3 Common avionics designs used for CS, CTV, and US	1.3 Level of modularity and common design approach is? (to LRU level, or sub LRU)	1.3 What does MSFC mean by common avionics designs?
2.1 Reusable avionics for CPAK and CTV	2.1 Expendable avionics for (CPAK)	2.1 Issues: nonrecurring cost to achieve portability, common design, maintenance support
2.2 Expendable avionics for CS and US	2.2 Reusable avionics for CS and US	2.2 Issues: Recurring cost of hardware, verification and validation of flight hardware
2.3 Fail-operational (FO) minimum for all avionics flight control functions other than proxops	2.3 FO/FS minimum configuration	2.3 Issues: launch weight, system reliability

Advanced Avionics
Johnson Space Center

NLS Vehicle Flight Avionics—Modular Avionics Assessment (continued)

Preliminary Requirements	Tradeoffs	Comments
3.0 Fixed F/T architecture	3.0 Scalable F/T architecture (FO-FO/FO) provided for upgrade	1.1 Issues: extensibility of the hardware; nonrecurring costs higher
4.0 Fault masking during flight	4.0 Fault detection, isolation and recovery provided	4.0 Probability of mission success is lower if fault is masked (complexity of FDIR hardware could lower reliability also)
5.0 Grade 1 parts (class S)	5.0 Grade 2-plus parts; best available from grade 1 and grade 2-plus parts	5.0 No rework at wafer and wire bond level (grade 1) vs. rework allowed (grade 2); extensive burn-in test and hermetic seal vs. less burn-in and polymer seal
8.0 Off-the-shelf design	8.0 New hardware design	8.0 Nonrecurring costs; technology, maturity
9.0 Passively cooled avionics	9.0 Actively cooled avionics	9.0 Launch weight, survivability
10.0 Standard data bus 1553/copper	10.0 Optical data bus (HSDB, FLBH)	10.0 EMI immunity, system bandwidth and growth, launch weight (COTS)
11.0 Separate buses for flight critical data	11.0 All data types on same bus/network	11.0 System fault contamination, autonomy (fail-op, voting)

Honeywell

Systems and Research Center

Advanced Avionics
Johnson Space Center

NLS Vehicle Flight Avionics—Modular Avionics Assessment (continued)

Preliminary Requirements	Tradeoffs	Comments
12.0 Standard software language—ADA for flight software	12.0 "C" or "C++" language	12.0 Robustness of language, portability, flight qualification
13.0 Distributed processing architecture	13.0 Centralized processing	13.0 System reliability
14.0 Common 32-bit standard processor	14.0 16-bit (1750A) standard processor, 64-bit standard processor; processor family	14.0 System growth extensibility (Rad-hard)
15.0 Common processor in each subsystem	15.0 Different processors allowed in subsystems	15.0 System cost
16.0 Engine-out capability	16.0 No engine-out capability	16.0 System reliability
17.0 Propulsion module expendable	17.0 Propulsion module is recovered (partially and entirely)	17.0 Lower nonrecurring cost initially (simpler design), lower launch weight (nonreusable, less need for IHM)
18.0 Maximum G level is 4.5 G	18.0 Manned vs. unmanned flights	18.0 Survivability of avionics

Advanced Avionics
Johnson Space Center

B-44

Missions

Advanced Avionics
Johnson Space Center

Missions

- Earth to orbit
  - Space Transportation System (STS)
  - Space Transportation System–Cargo (STS-C)
  - Expendable (Titan, Atlas, Delta, other)
  - Heavy Life Launch Vehicle (HLLV)
  - Advanced Launch System (ALS)
- Transfer
  - Orbital
  - Lunar
  - Mars
- Excursion
  - Lunar
  - Mars
- Orbital
  - Space Station Freedom (SSF)
  - Man-Tended Transportation Node (MTTN)
  - Exploratory Probe (Probe)
  - Personal Maneuvering Unit (PMU)
  - Orbital Maneuvering Unit (OMU)
- Surface
  - Lunar Module
  - Mars Habitation Module

8 - 4

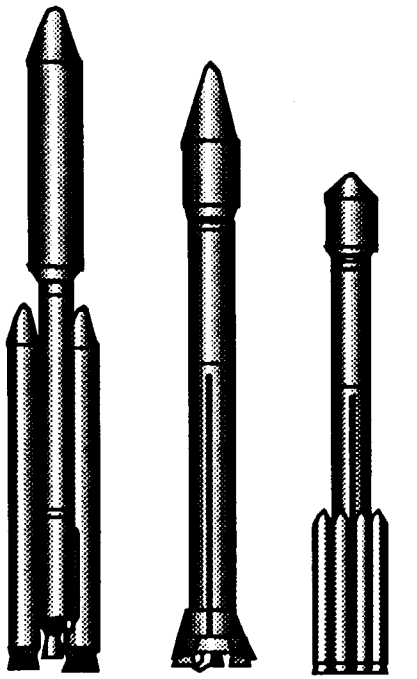
Advanced Avionics
Johnson Space Center

Vehicles

Expendable and Shuttle-Derived Launch Vehicles

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

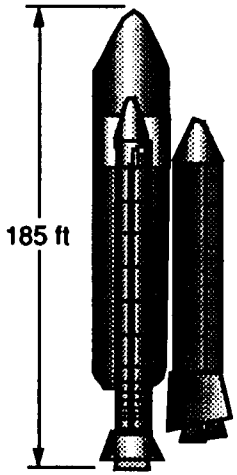


Titan IV
39–50K
Payload

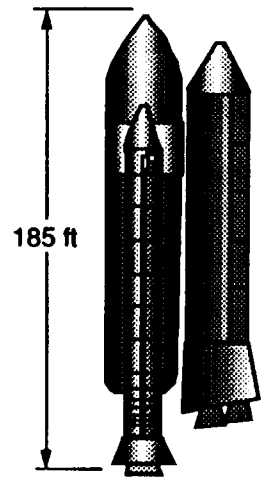
Atlas II
15–20K
Payload

Delta II
9–11K
Payload

Expendable Launch Vehicles (ELVs)



Net Payload	175K
Boosters	2 ASRBs
Core Stage	Standard ET
Core Propulsion	3 SSMEs
Payload Envelope	15-ft dia., 82-ft length



Net Payload	135K
Boosters	2 ASRBs
Core Stage	Standard ET
Core Propulsion	3 SSMEs
Payload Envelope	25-ft dia., 90-ft length

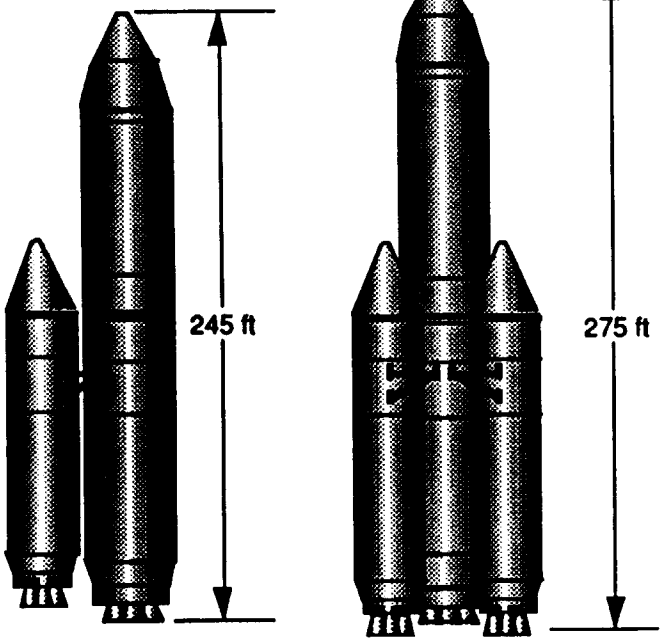
Shuttle-Derived Vehicles for LEO and Lunar Missions

Source [AUST89]

ALS and HLLV Vehicles

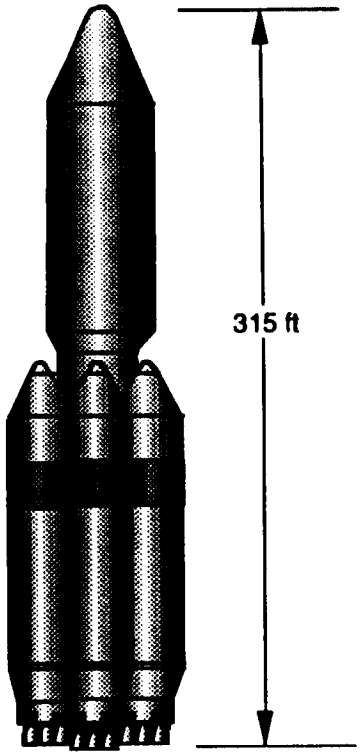
COTS FOR SPACE

Advanced Avionics
Johnson Space Center

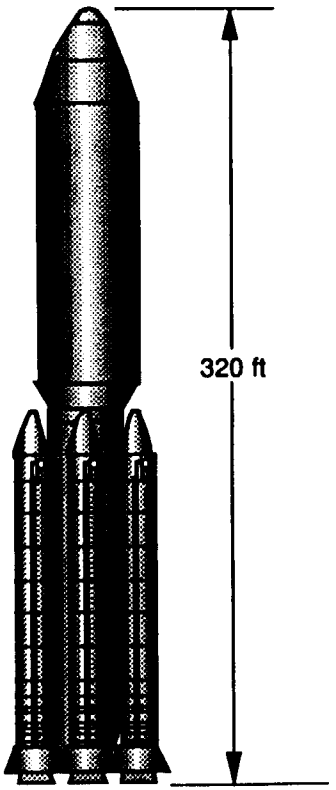


Net Payload	115K
Boosters	3 LOX/LH_2 with 6 STMEs ea.
Core Stage	LOX/LH_2
Core Propulsion	3 STMEs
Payload Envelope	25-ft dia., 100-ft length

Net Payload	215K
Boosters	2 LOX/LH_2 with 6 STMEs ea.
Core Stage	LOX/LH_2
Core Propulsion	3 STMEs
Payload Envelope	40-ft dia., 100-ft length



Net Payload	300K
Boosters	3 LOX/LH_2 with 6 STMEs ea.
Core Stage	LOX/LH_2
Core Propulsion	3 STMEs
Payload Envelope	40-ft dia., 100-ft length



Net Payload	300K
Boosters	4 ASRBs
Core Stage	New 30-ft dia.
Core Propulsion	Recoverable P/A with 5 SSMEs
Payload Envelope	40-ft dia., 100-ft length

Source [AUST89]

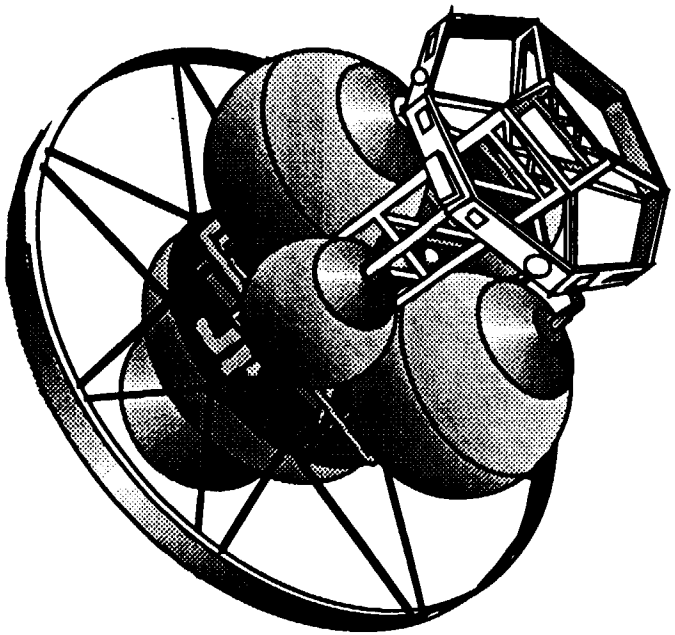
Honeywell

Systems and Research Center

C910929-69

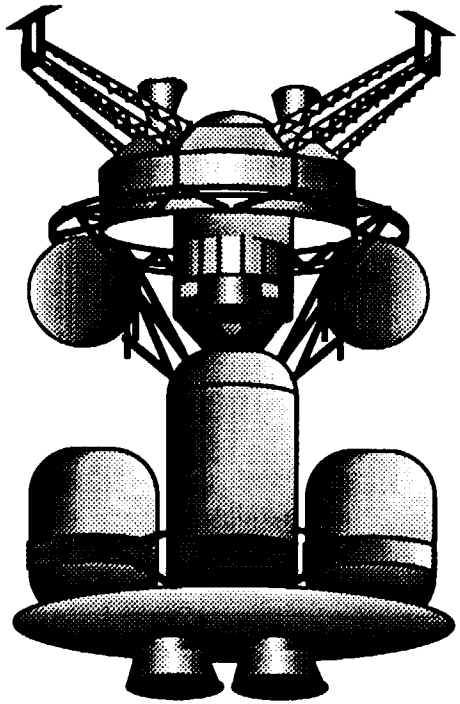
Advanced Avionics
Johnson Space Center

Orbital Transfer and Lunar/ Excursion Vehicles



Orbital Transfer Vehicle

Source [ORBI85]



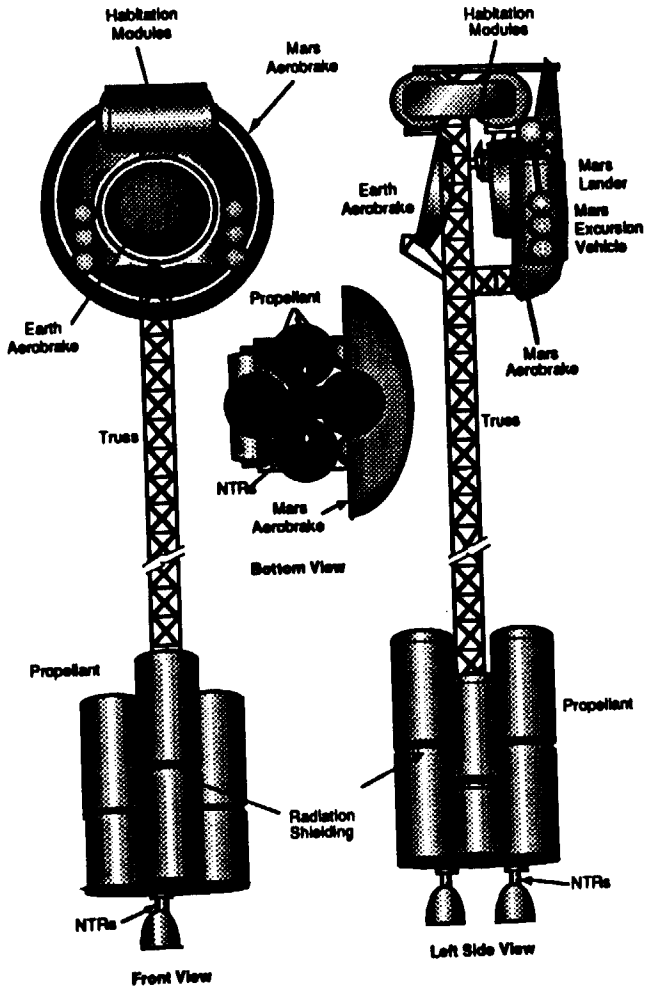
Lunar Transfer and Excursion Vehicle

Source [AUST89]

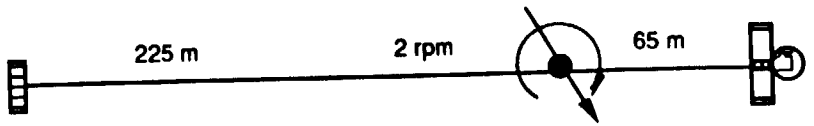
Mars Transfer Vehicle
Design II

COTS FOR SPACE

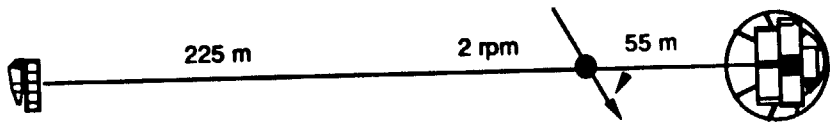
Advanced Avionics
Johnson Space Center



Inbound Artificial Gravity Configuration



Outbound Artificial Gravity Configuration



Power Systems
- 50 kWe Stirling Engine (100 kg mass)
- 25 kWe fuel cell backup systems

Thermal and Radiation Protection
- In-flight
  - Hydrogen propellant tanks
  - 0.089-m Al skin
  - MTV radiation protections
  - Mars entry: Aerobrake

Life-to-Drag Ratio
- 0.3 for α = 18 deg

Center of Gravity
- TMI: 19.3 x 21.85 x 16.75
- Post-TMI: 19.3 x 21.85 x 11

Operational Purpose
- Transportation of landing vehicle and astronauts from low-earth orbit to Martian orbit

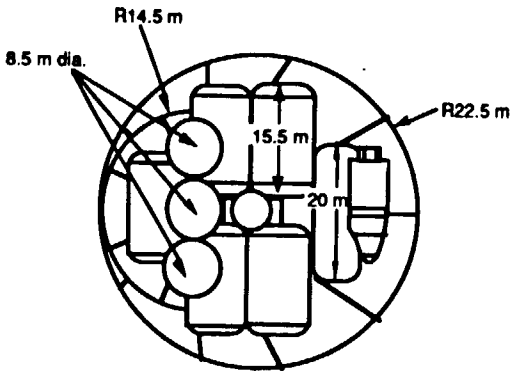
Source: University of Minnesota Space Research Association

Honeywell

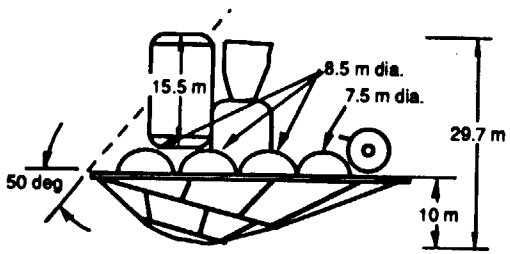
Systems and Research Center

Mars Transfer Vehicle
Design I

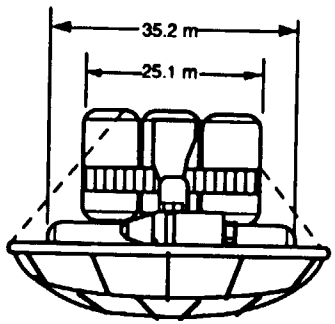
Advanced Avionics
Johnson Space Center



Top View



Side View



Rear View

Mass
- 352 t (dry)
- 911 t (wet) TMI
- 632 t (wet) for use during artificial gravity

Dimensions (m)
- Aerobrake: 45 x 45 x 10
- TMI: 45 x 45 x 29.7
- Post-TMI: 45 x 45 x 29
- Crew quarters: 20 x 5.9 x 4.75 (2.4 per level)

Trip Time
- Outbound: 175 days
- Inbound: 249 days

Endurance
- Life sustaining: 484 days
- Structural: current components with exception of AFE aerobrake are reusable

Main Engine
- Pellet-bed nuclear thermal rocket
- Thrust: 1112 kN during TMI, 667.2 kN post-TMI

Propellant
- Liquid hydrogen
- Propellant mass: 539 t
- Propellant volume: 67699 m^3 (total)

Reaction and Control Systems
- Orbital maneuvering system
- Main engine throttle down (for orbit transfer and orbit correct)
- Altitude control system
  - Gaseous H^2, 0^2
  - 36 thrusters
  - 14.87 t propellant
  - 0.2 metric pressurant mass
  - DV = 0.104 km/s for maneuvering

Communication Systems
- Ka-band at 32 GHz
- 5-m collapsible dish antenna
- Two racking data relay satellites (TDRS)

Navigation Systems
- Space sextant
- Three IMUs with MGSS and TDRS assistance

Tether Systems
- 2 rpm in order to sustain 9.8 m/s^2 or 1 G, for artificial gravity
- Outbound length: 280.8 m cg to cg
- Inbound length: 275.4 m cg to cg
- Tether composition:
  - Kevlar 49
  - 0.03-m-dia. cable
- Tether mass: 2.43 t
- Gravitational gradient: 9.8367 • g • 9.5033 m/s^2

Source: University of Minnesota Space Research Association

Mars Excursion Vehicle

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

Mass
- 40.1 t (dry)
- 87.8 t (wet)
- Ascent
  - 18.7 t (dry)
  - 61.9 t (wet)

Dimensions (m)
- 15 x 5.6 x 5.6
- Ascent stage: 5.8 x 5.4 x 7.4
- Crew quarters: 2.2 x 6.5 x 6.5

Endurance
- Life sustaining: 7 days
- Structural: nonreusable

Main Engines
- Descent 3: Pratt & Whitney RL 10–IIb
- Ascent 3: Pratt & Whitney RL 10–IIb
- Thrust
  - Descent: 39.6 kN
  - Ascent: 198 kN

Operational Purpose
- Transportation between Mars orbit to and from the MHM

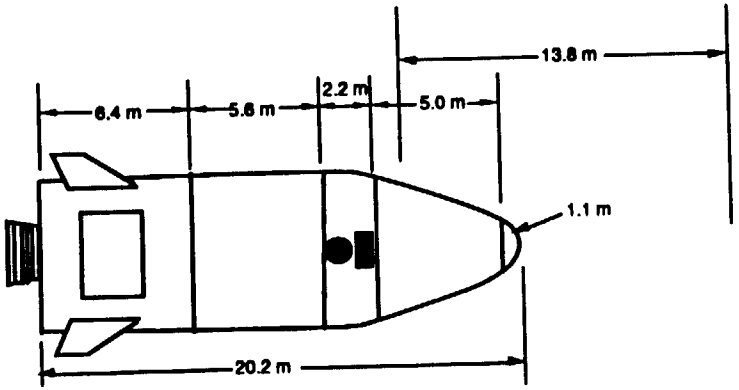
Trip Time
- Descent stage: 8 h
- Ascent stage: 10 h

Reaction and Control Systems
- Nitric tetric oxide
- Mono-methal
- Hydrazine: Parachutes drogue chute to adjust to vertical attitude

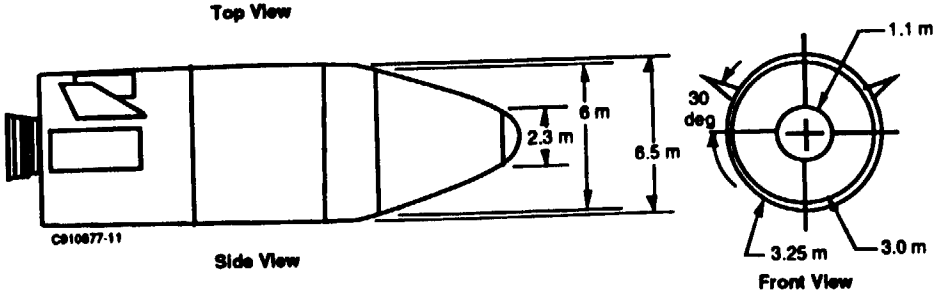
Communication Systems
- Short-band radio, K band

Navigation Systems
- IMUs

Radiation Protection
- In-flight biconic shape
- Life-to-drag ratio: 1.0 for α = 28 deg



Top View



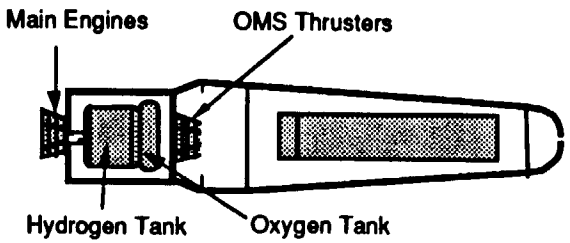
Side View

Front View

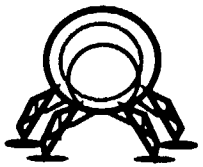
Source: University of Minnesota Space Research Association

Mars Habitation Module
Design I

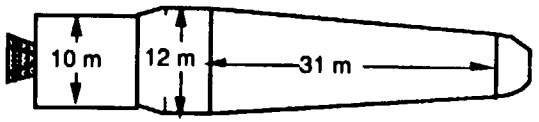
Advanced Avionics
Johnson Space Center



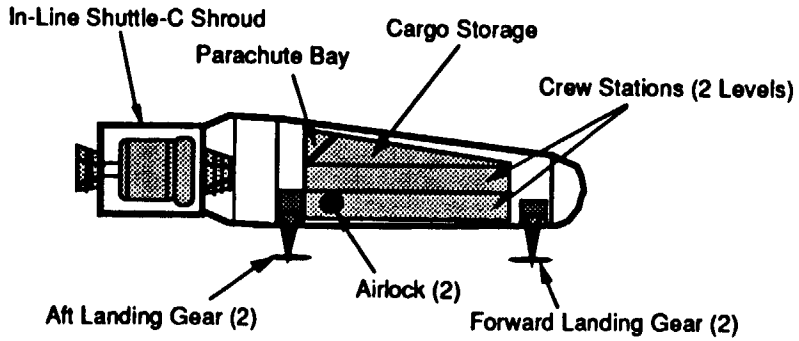
Top View



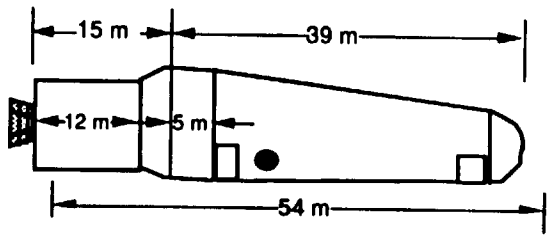
Front View



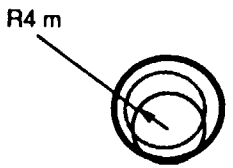
Top View



Side View



Side View



Front View

MHM Component List

- One 12-m-dia. x 40-m raked biconic shell
- One 5.9-m-dia. x 25-m crew quarters
- Three OMS thrusters
- Three main ET/STME engines
- One 8.5-m-dia. x 6-m hydrogen fuel tank
- One 8.5-m-dia. x 2.2-m oxygen fuel tank

Scale: 1:800

Source: University of Minnesota Space Research Association

Advanced Avionics
Johnson Space Center

B-59

Environments

Advanced Avionics
Johnson Space Center

Avionic Sensitivities to Mission Environments

	Launch and Re-entry	Earth Satellite	Deep Space	Lunar Landing and Relaunch	Planetary Landing and Relaunch	Component Improved Environment
• Thermal						
Heat Flux	☒	☒	☒	☒	☒	
Thermal Shock	☒				☒	
Temperature	☒	☒	☒	☒	☒	X
• Radiation						
Van Allen		☒	X		☒	
Cosmic		X	X			
Artificial		☒	X	X	X	
Solar		☒	X	☒	☒	
• Solid particle						
Dust Clouds		X	X	X		
Meteoroids		X	☒	X		
• Vacuum	☒	☒	☒	☒	☒	
• Mechanical Acceleration						
Vibration	☒	X	X	X	☒	☒
Shock	☒			X	X	☒
Accelerations	☒	X	X	X	X	X
Zero G		X	X			
Acoustics	☒					

☒ Extremely important in design

Source [LEKU64]

Advanced Avionics
Johnson Space Center

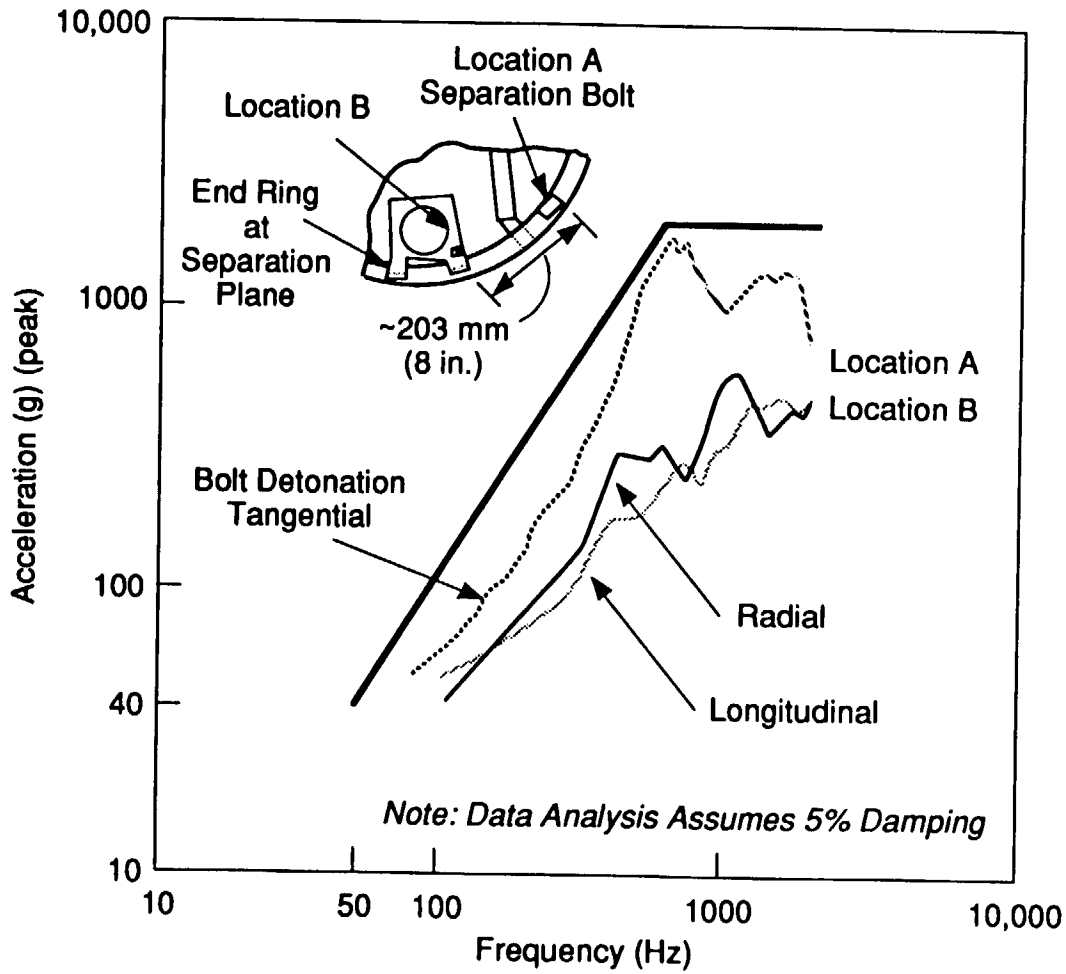
Radiation Effects and Hardening Technologies

	Effect	Natural Radiation		
		Source of Effect	Critical Components	Hardening Techniques
Permanent	SEU/Latchup	• Cosmic radiation • None*	• CMOS memory	• Hardened parts (EPI)
Permanent	Total Ionizing Dose	• Electrons and protons (cum) • X-ray/gamma rays*	• All active devices	• Part selection • Shielding • Location
Permanent	Dislocation (bulk) Damage	• Protons (cum) • Neutrons (cum)*	• Transistors • Linear devices	• Part selection • Shielding • Location
Permanent	Dose Rate (latchup)	• Heavy particles • X-rays/gamma rays*	• CMOS • CMOS*	• Hardened parts (EPI, SOS) • High-Z shielding* • Current limiting* • Circumvention*
Permanent	Dose Rate (burnout)	• None • X-rays/gamma rays*	• N/A • All active devices*	• N/A • High-Z shielding* • Current limiting* • Circumvention* • Part selection*
Transient	Single-Event Upset (SEU)	• Cosmic radiation and protons • N/A*	• CMOS memory • None	• Hardened parts • EDC • Part selection • Error detection
Transient	Dose Rate (upset)	• None • X-ray/gamma ray*	• N/A • All bistable circuits* • High-Z shielding* • Circumvention* • Part selection*	• None • High-Z shielding* • Circumvention* • Part selection*

* Applies only to man-made effects.

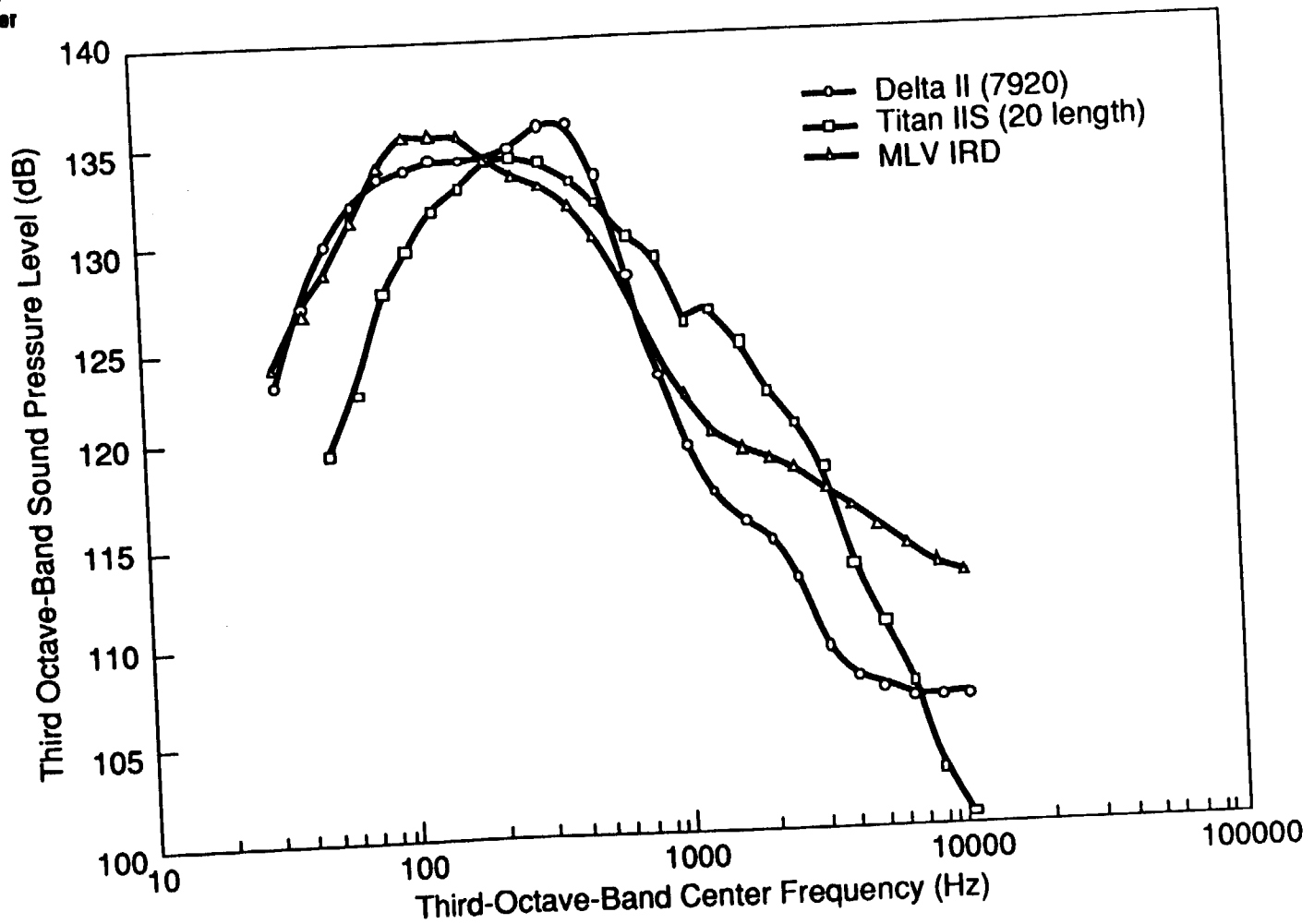
Source: Adapted from [ORB185]

Delta Spacecraft Separation Shock Data (5414 fitting)



Source [GRIF91]

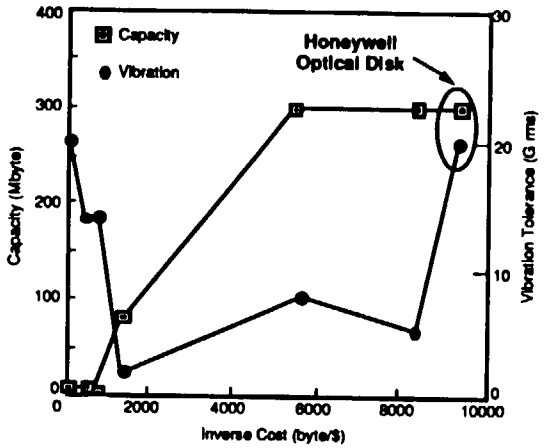
Fairing Internal Acoustic Environment

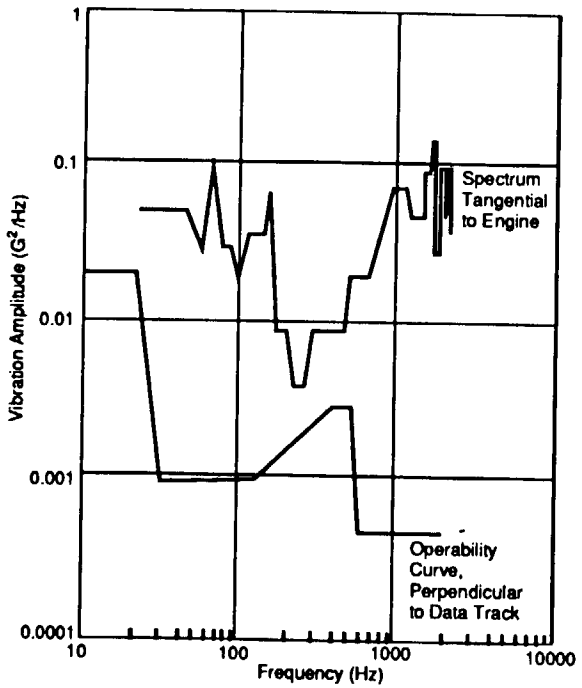


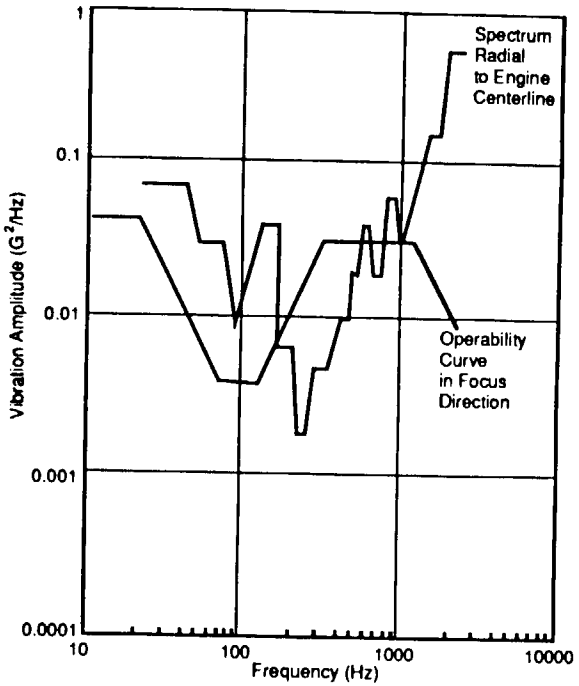
Source: Personal Communication from Space Applications Corporation

Optical Disk Vibration Tolerance

Advanced Avionics
Johnson Space Center







Advanced Avionics
Johnson Space Center

B-66

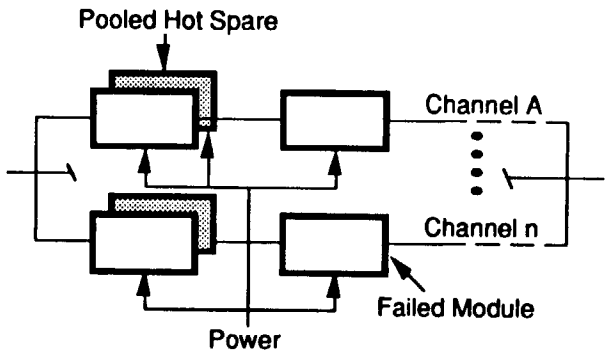
Specifications

Ultra-Reliability Requirement Implementation

Advanced Avionics
Johnson Space Center

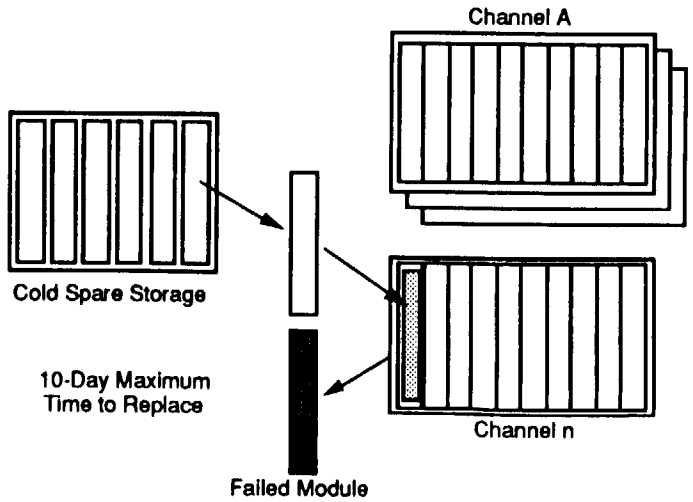
Problems

- Ultra-reliable avionics are desirable for extended and deep-space missions. These missions will degrade avionic reliability due to increased galactic and solar radiation exposure.
- Ultra-reliability (fail-op, 10 failure probability) may not be practical to meet. This normally brings up fault tolerance, fault detection, fault isolation, and recovery (FDIR) design issues.
- Parallel redundancy and/or pooled sparing redundancy using multipurpose electronics modules will be required for longer duration missions. The cost to orbit and posit powered redundant avionics is undesirable.



Solution

- Define architecture to allow cold sparing and hot/cold insertions
- Define new deferred maintenance architecture (e.g., quad channel) and operations (e.g., <10-day deferral) for cold sparing. In this solution, maintenance is used for cold spare insertions. This eliminates the cold spare technology gap identified in other studies.
- Specify cold storage in areas other than user chassis (may be protected storage areas)

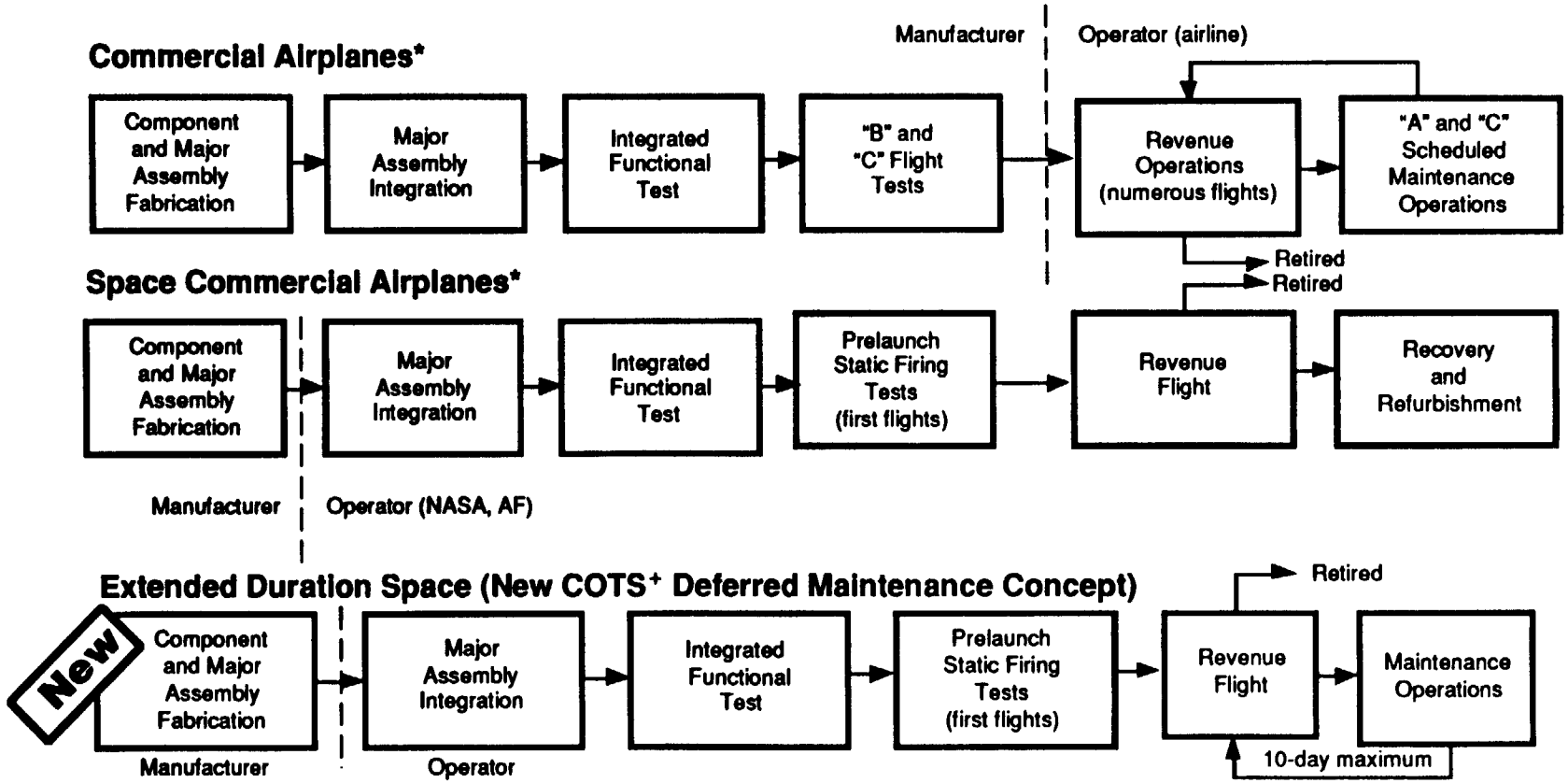


Benefit

- Ultra-reliable reliability
- No technology gap

Advanced Avionics
Johnson Space Center

Manufacturing and Maintenance Operations



* M. Raftery, Boeing "The Application of Commercial Airplane Avionics to Advanced Space Transportation," AIAA 90.

Launch System Requirements

1. *Reliability*: Performance (MTBF, environment), BIT, use of expert system, distributed test & fault isolation

2. *Maintainability*: packaging, modularization, VHSIC, local maintenance

3. *Autonomy*: ground checkout & integration, quick turnaround, launch readiness assessment

4. *Autonomous Integrated Flight Control*: autonomous near real-time system/subsystem reconfiguration in response to faults

5. *Guidance, Navigation, & control*: autonomous to adapt to faults & variations in environment

6. *Low operational costs*: standard common modules, replaceable modules, integrated avionics/ground support

7. *Health monitoring*: automated on board prelaunch checkout, inflight monitoring, redundancy management, maintenance system activity scheduling, eliminate vehicle ground inspection activity, fault avoidance, used to obtain a diagnosis of potential system failures to increase system availability, on-board data compression

8. Monitor, analyze, and archive LRU data

9. Monitor performance in test

10. Determine flight readiness

11. Monitor performance in flight

12. provide for interactive operator participation

13. Analyze & report post-test & post-flight

14. Fault Tolerance Requirements:

    •Provide avionics & power systems which are failure-free to the extent required by flight mission reliability

    •There shall be no maintenance activities post-rollout

    •assume TBD failure rates & system operating times

    •with a post-factory checkout failure of any LRU, meet the mission reliability req, i.e. fly with a failed LRU

+ From integrated Health Monitoring study (Avionics, propulsion, Engine, EMA)
* Sources: MSFC/HLVC, ICS, MDAC ALS, MPRAS

- Fault tolerant methodology should consider use of existing (COTS) software and should be compatible with use of distributed digital systems, common hardware, and growth capability

15. *Maintainability*: Simple, reliable, Standardized design (i.e. standardized interfaces)

16. Adaptive Flight Operations (launch in maximum weather conditions with adaptive GN&C and predictive health management function

17. *Automated*: Req analysis, design, manufacturing, assembly, test, inspection, in for integration, mission planning, ground processing, logistics, records management, access to design & manuf.. data

18. Manuf. & assembly completed prior to launch site processing

19. Standardized & minimized ground operations (to accommodate all aspects of mission req envelope, minimize steps & complexity of ground ops)

20. *Flight & Ground software*: procedural language (i.e. Ada), conventional real-time software on vehicle only, use expert system to replace standing army, common software modules, common protocols

21. Incorporate Health Management to minimize on-board complex logic

22. Provide system status information during health and redundancy management, acceptance, integration and checkout

+ From integrated Health Monitoring study (Avionics, propulsion, Engine, EMA)
* Sources: MSFC/HLVC, ICS, MDAC ALS, MPRAS

Advanced Avionics
Johnson Space Center

Fault Tolerance Requirements Issues

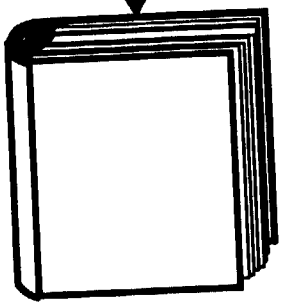
- Systems must be partitioned to separate critical, essential, and nonessential functions
- Critical fault-tolerant systems must use redundancy and the redundant components must be independent and contained within fault containment areas
- It may not be economical to contain and isolate all possible faults from propagating among all parts of the system
- Fault tolerance requirements should be such that some faults are contained as close as possible to the originally faulty part while other fault effects may be allowed to escape to other components; however, the propagation of all faults must be contained at some point

Requirements Documentation

Advanced Avionics
Johnson Space Center

Mission Definition

- Functional requirements
- Performance requirements
- Environmental requirements
- Operational and maintenance requirements
- Cost



System Requirements Specification (SRS)

Mission • Vehicle – Avionics	Duration	Operations	Acceleration	Shock	Pressure	Radiation	Acoustic	Temperature
Earth to orbit • STS – Avionics • STS-C – Avionics • HLLV – Avionics • NDV – Avionics								
Transfer • LTV – Avionics • MTV – Avionics								
Orbital • SSF – Avionics • OMU – Avionics • MTTN – Avionics • PMU – Avionics								
Excursion • LEV – Avionics MEV – Avionics • Probe								

Mission • Vehicle	Logistics	Performance	Reliability	Availability	Vibration	Opportunity	Launch	Landing	EMI

Mission • Vehicle	Humidity	System Safety	No. of Personnel	Man Machine	Maintainability	Fault Tolerance	Coverage

Requirements Summary

Honeywell

C910929-80

Advanced Avionics
Johnson Space Center

Space Station Freedom Requirements

♦ Mission • Vehicle - Avionics	Maintainability	Safety	Autonomy	Cost	Testability	Security	Electromagnetic Interference	Growth & Flexibility	Particle Contamination		
♦ Orbital • SSF - Avionics	Permit repair or replacement at the ORU level. Provide facilities and equipment for on-orbit monitoring, checkout, storage, replacement, repair, and test. Critical systems shall be capable of undergoing maintenance without the interruption of critical services and shall be "fail safe" while being maintained. Design for easy removal, repair and replacement to the lowest level practical	Removal of hazard sources and operations Selection of least hazardous design or operations Safety factors, containment, isolation, purge, redundancy, backup systems, workarounds, safety devices, caution and warning devices, and procedures Maintainability program and adherence to maintenance and repair schedules	Minimize crew and/or ground involvement in system operation	Minimize operations-driven costs and maximize effectiveness for users	Provide access to test points Support EVA test and checkout	Command and data handling system shall be capable of secure communications as required for normal and emergency operating conditions Secure voice/video communications shall be provided between crew and ground Payloads responsible for their own command and data encryption	Meet normal manned-space-flight standards	Initial hw/sw shall be capable of being replaced or integrated with higher technology systems as they become available in areas anticipated to provide economical growth in capability	Hermetic seal		

Advanced Avionics
Johnson Space Center

Space Station Freedom Requirements

♦ Mission • Vehicle - Avionics	Operations	Duration	Acceleration	Acoustics	Vibration	Shock	Pressure	Temperature	Radiation	Reliability	Modularity
♦ Orbital • SSF - Avionics	Prelaunch, launch, deployment, construction, servicing experiments and facilities including payloads and satellites, test and deployment of payloads and upper stages, national security operations, large-scale construction of space structures	30 year mission subsystems: 10 year minimum using maintenance as necessary	Same as launch vehicle	Same as launch vehicle	Same as launch vehicle	Same as launch vehicle Docking impact	Shirt-sleeve, nitrogen-oxygen environment at pressure selected to facilitate productive EVA with no pre-breathing or other operational constraints	200° K during darkness to 350° K in direct sunlight Provide internal conduction paths to avoid damage due to temperature differences between sunlit and dark sides	Figure 1 illustrates the radiation environment for various near earth orbits A permanent platform may encounter doses up to 3,000 Mrad	SSF critical: FO/FS/restore Mission critical: FS Redundant functional paths to permit verification of operational status in flight w/o removal of ORUs Instrumented for the detection and isolation of failures to the ORU level	Common hw, sw, and technology to enhance standardization for direct interchangeability assure compatibility, and minimize program development costs

Advanced Avionics
Johnson Space Center

Lunar Transfer Vehicle Requirements

♦ Mission • Vehicle - Avionics	Maintainability	Safety	Autonomy	Cost	Testability	Security	Electromagnetic Interference	Growth & Flexibility	Particle Contamination		
• LTV - Avionics	Provide facilities and equipment for monitoring and checkout Design for easy removal, repair and replacement to the lowest level practical	Manned vehicle safety design requirements	Minimize ground support	Minimize operations-driven costs	Provide access to test points Support ground and Lunar test and checkout	Payloads responsible for their own command and data encryption	MIL-STD-1541 Meet normal manned-space-flight standards	Flexibility to meet the needs of various payloads	Hermetic seal Lunar soil accumulates and acts as a thermal insulator		

Advanced Avionics
Johnson Space Center

Lunar Transfer Vehicle Requirements

♦ Mission • Vehicle - Avionics	Operations	Duration	Acceleration	Acoustics	Vibration	Shock	Pressure	Temperature	Radiation	Reliability	Modularity
♦ Transfer • LTV - Avionics	Prelaunch; launch; deployment; SSF docking; Lunar transfer, orbit, landing, prelaunch and launch; Earth transfer	30 days	69 m/s^2	Figure 24 provides data for the acoustic environment for the 7920 and 7925 vehicles (10 ft diam fairing). Levels for the 6920 and 6925 vehicles are 0.5 dB less	Same as launch vehicle	Same as launch vehicle	Figure 25 illustrate the atmospheric pressure bleed-down rate during ascent	Figure 26 provides typical maximum temp profiles at the inner wall of the 6920 and 7920 vehicle fairing acoustic blanket Maximum temp due to lift off is approximately 150° F Maximum aerodynamic heating for payload after shroud separation is 1135 W/m^2	Figure 27 illustrates electron dose vs aluminum shield thickness for deep space	Figure 28 provides a reliability vs. mission time profile On-board checkout, fault detection, and isolation	Commonality and modularity to reduce costs and spares provisioning, optimize functional interfaces and sw module allocation

Advanced Avionics
Johnson Space Center

Heavy-Lift Launch Vehicle Requirements

• Mission • Vehicle - Avionics	Operations	Duration	Acceleration	Acoustics	Vibration	Shock	Pressure	Temperature	Radiation	Reliability	Modularity
• Earth to Orbit • HLLV - Avionics	Prelaunch, launch, payload support, refurbish	20 missions Some reusable components	Linear: +/- 20 g max, angular: +/- 100°/sec^2 Figures 5-8 illustrate Delta and Titan acceleration and shock data	139 dB is the current NASA acceptance for inertial upper stage components 155 dB MPRAS requirement Acoustic environment data from inside Delta II (7920), Titan IIS and MLV IRD are illustratnd in Figures 9-11 Table 1 provides Titan acoustics data	11 Grms Figures 12-18 provide vibration environment data for Ariane, Atlas-Centaur, Delta, and Titan vehicles	Figures 5-8 illustrate Delta and Titan acceleration and shock data 10 g landing, 1,000 g separation	10^{-10} Torr to 18 psia Outgassing limits of NASA SP-R-0022A, thermal-vacuum tests. Table 2 provides pressure, temperature and density data for altitudes from 0 to 400 km	Operational: -65° F to 160° F Non-operational: -65° F to 200° F	4 Rads (Si) Proton flux due to solar wind in earth's orbit is about 10^9 P cm^2/sec with energies between 1 and 3,000 electron volts (ev). Electron flux may be as high as 10^{10} e/cm^2/sec with energies less than 2 ev.	0.999 to support launch reliability of 0.98 or higher (launch on schedule probability of at least 0.95) See Figure 19 for illustration of number of missions vs. cost for various probability of success values.	Hardware and Software, standardization of interfaces and data busses MIL-HDBK-246A, Program Managers Guide for the Standard Electronic Modules Program

Advanced Avionics
Johnson Space Center

Heavy-Lift Launch Vehicle Requirements

• Mission • Vehicle - Avionics	Maintainability	Safety	Autonomy	Cost	Testability	Security	Electromagnetic Interference	Growth & Flexibility	Particle Contamination		
• Earth to Orbit • HLLV - Avionics	Provide facilities and equipment for prelaunch, inflight, or refurbishment monitoring and checkout Design for easy removal, repair and replacement to the lowest level practical	Range safety Man-rated safety design requirements	Require far less launch support than current systems	ALS program goal: 10 fold cost reduction (current costs range from $5,000 to $10,000 per kilogram)	Parts and components qualification testing: SMASO STD 73-2C, MIL-STD-1540A See Figures 20-23	Secure communications and data transmission and reception over various RF links are encrypted	MIL-STD-1541 Meet normal manned-space-flight standards	High degree of flexibility to meet operational needs Accommodate changes in mission parameters late in the prelaunch sequence	Hermetic seal		

Cost (TBD)

Low cost

Reliability

nominal mtbf	high rel mtbf	ultra rel mtbf
15,000 hrs	30,000 hrs	150,000 hrs
(class B)	(class S)	(order of mag. improvement)

Component (module) reliability, nominal estimate based on supplier MIL-HDBK-217, common module reliability calculations. Assumptions: missile launch environment, 50 deg C at card edge, class B parts

Maintainability

Vehicles operating in a space environment must utilize built in test and fault isolation to track faults to single (or small number of) replaceable modules. Equipment must be spacesuit compatible without tools and should include handholds for leverage on zero g class vehicles.

Useful Life

Earth to orbit: 1 - 200 hours (8.3 days), up to 720 hours (30 days), reuses = 0, 50-250
Transfer/Excursion vehicles:
- Lunar: 200 - 2,000 hours (8.3 - 83.3 days), 4 days excursion, 30 days transfer, reuse = 5 missions/life
- Mars: 12,000 - 35,000 hours (500 days - 4 years), 600 days excursion, 1100 days transfer, reuse = 1 use for chemical vehicle concept, 2 uses for nuclear vehicle concept

Orbital platforms: 85,000+ hours (10+ years)
- Personal maneuvering units: 12 hours, 5 year life
- Orbital maneuver and cargo transfer: 30 days
- SSF exploratory probes: 10 years, single use per life

Mobile planetary systems: 1 day - 3 months, 5 year life
Fixed planetary systems: 20+ years

Safety (TBD)

Quality Assurance (TBD)

Transportability (TBD)

Health Monitoring (TBD)
- **architecture**
- **percent coverage**
- **detection**
- **isolation**

Commonality (TBD)
- **interchangeability**
- **standardization**

Environmental (TBD)

- **Acceleration**

The highest acceleration is expected to occur during the Earth to orbit (ETO) mission segment or during aerobraking and re-entry. Shuttle launch produces up to 4 g of dynamic acceleration.

- **Vibration**

The most severe vibration occurs during the ETO mission segment or during aeromaneuvering.

- **Shock**

Shock events are associated with the following mission events: staging, docking, maneuvers, landing, or emplacement.

- **Electromagnetic** (TBD)

- **Thermal**

Based on information provided by the Lunar Transportation Facilities and Operations Study Final Report by McDonnell Douglas, Lunar surface temperatures range from -153 °C at night to 108 °C in daylight. The average Earth's surface temperature is about 22 °C. Equipment utilized on the moon will be exposed to a solar radiation heat load of up to 442 BTU/hr/ft^2.

Alternate information about thermal exposures for the Lunar orbits as well as Earth and Mars orbit is provided by the Boeing report:

Within planetary atmosphere - specify vehicle/system temperature
In orbit - specify heat flux/thermal radiation from sun and nearby planet
LEO = Low Earth Orbit
LLO = Low Lunar Orbit
LMO = Low Mars Orbit

LEO: 200 W/m^2 in earth's shadow and 1600 W/m^2 when exposed to sunlight.
LLO: 15 W/m^2 in moon's shadow and 2800 W/m^2 when exposed to sunlight.
Venus fly-by: 2800 W/m^2
LMO: 110 W/m^2 in Mars' shadow
Mars surface: -95° C to 25° C

- **Contamination (Dust)**

The Lunar Transportation Facilities and Operations Study identifies dust as a major design consideration. The Lunar dust has low electrical conductivity which allows it to build up an electrostatic charge. The charged dust particles are then likely to be attracted to and stick to surfaces of bodies in their immediate proximity. The layered dust poses risk both as a contaminant and as an insulating blanket which impedes heat dissipation from electronic equipment.

- **Meteorite**

Code Z 1989 Exploration Study Requirements Document provides a requirement for micrometeoroid protection for flight vehicles while on the Lunar surface. The phenomenon has been quantified in the following equation:

$Log_{10}N_{sp} = -14.41-1.22\ log_{10}m$ where,

N_{sp} = number of particles of mass m or greater per square meter per second
m = particle mass in grams

According to this equation for estimation, a vehicle on the Lunar surface with 250 m^2 of surface area will experience 750 strikes per year by a meteoroid of 10^{-6} grams or more. The vehicle must be provided with protection to assure a probability of 0.985 against penetration over thirty years. Space Station Freedom currently has a protection prevision requirement of 0.9995 probability of no micrometeoroid penetration per year.

- **Radiation**

The space radiation environment is composed of three main components: earth's trapped radiation belts, galactic cosmic rays, and solar cosmic rays. On-board nuclear power reactors are an additional potential source of radiation. Radiation effects can be transient (single event upset) or permanent (total dose, displacement damage, latchup, burnout). Techniques for hardening to long-term effects include: shielding, device selection, device hardening, and electronics design margin (fault tolerant design for single event upset and examination of effects on critical parameters of each device/module). About 40 - 60 mils of Al is recommended for radiation shielding of electronic equipment (approximate from Boeing chart).

Galactic cosmic ray exposure on the Lunar surface has been quantified in the following ways:

1.3×10^8 to 7×10^7 protons/cm^2 with energy levels between 40 and 10^{13} MeV.

The equivalent average annual dose is 12 REM.

Solar proton events lead to radiation energy levels in the order of 3 to 300 MeV. It is likely that solar storm shelters will be used on the Lunar surface to protect personnel and equipment from the previously detected solar storms.

Advanced Avionics
Johnson Space Center

B-84

Architecture

Advanced Avionics
Johnson Space Center

B-87

Architectural Functions

B-89

Avionic Functions Addressed

Advanced Avionics
Johnson Space Center

Avionic Functions	Candidate Systems			
	Earth to Orbit	Transfer/Excursion	Orbital	Study Reference
	STS STS-C HLLV NDV	LTV MTV LEV MEV	PMU OMV SSF MTTN Probe	
Guidance and Navigation	x x x x	x x x x	x x x x	x
Flight Control/Effectors	x x x x	x x x x	x x x x x	x
Propulsion/Fluids	x x x x	x x x x	x x x x x	x
Telemetry	x x x x	x x x x	x x x x	
Communication	x x x x	x x x x	x x x x x	x
Power Management	x x x x	x x x x	x x x x x	
Data Acquisition	x x x x	x x x x	x x x x x	x
Data Management	x x x x	x x x x	x x x x x	x
Crew Support	x x	x x x x	x x	
Range Safety	x x x x			
Health Monitoring	x x x x	x x x x	x x x x x	x
Deorbit/Recovery	x x x x	x x		
Rendezvous/Docking	x x	x x x x	x x	
Payload Support	x x x x	x x x x	x	
Ground Support Equipment	x x x x			x

Adapted from "General Dynamics Space Avionics Requirements Study," Final Task Report, 10/30/90.

Avionic Function Definitions*

Guidance and Navigation
Process for achieving the desired conditions at engine cut-off and determing vehicle position and velocity.

Flight Control/Effectors
Process that commands vehicle actuators to achieve desired vehicle orientation, position, velocity, and acceleration.

Propulsion/Fluids
Process of determining fuel quantities and controlling fuel mixture and tank pressures for optimum vehicle performance.

Telemetry
Process for collecting sensor data from the vehicle and sending it via RF link to ground processing equipment.

Communications
Process of transmitting and receiving data, voice, and video signals between and within systems.

Power Management
Process of conditioning system power and routing it to subsystems in a controlled manner.

Data Acquisition
Process of sensing stimuli, converting to electrical signals, and providing signals to vehicle subsystems

Data Management
Processing, filtering, compression, handling and storage of data.

Crew Support
Provision for human interfaces, life support, and training and simulation.

Range Safety
Disabling or destroying a vehicle in the event of a failure which could result in injury or death.

Health Monitoring
Observation and recording of vehicle system status information and recommendation of reconfiguration response.

Deorbit/Recovery
Process of separating launch components for return to earth and control of attitude and position as required.

Rendezvous/Docking
Bringing vehicles and/or platforms together and coupling

Payload Support

*Adapted from General Dynamics Space Avionics Requirements Study, Final Task Report, 10/30/90 and Multipath Redundant Avionics Suite Reference Vehicle/Requirements, Preliminary, 6/7/89.

Interface with payload for basic support (e.g. power, processing), calibration, checkout and deployment.

Ground Support Equipment
Interface with ground equipment to provide resources and support during vertical integration, cargo and payload installation, and prelaunch phases of a mission.

Candidate Systems*

STS = Space Transportation System
STS-C = Space Transportation System - Cargo
HLLV = Heavy Lift Launch Vehicle
NDV = National Aerospace Plane (NASP) Derived Vehicle
LTV = Lunar Transfer Vehicle
MTV = Mars Transfer Vehicle
LEV = Lunar Excursion Vehicle
MEV = Mars Excursion Vehicle
PMU = Personal Maneuvering Unit
OMV = Orbital Maneuvering Vehicle
SSF = Space Station Freedom
MTTN = Man Tended Transportation Node
Probe = Exploratory Probe

The following systems are acknowledged, but not considered to be in the scope of this study:

Pressurized Surface Rover
Unpressurized Surface Rover
Robotic Surface Rover
Manned Soil Mover
Unmanned Soil Mover
Personnel Quarters
Command and Control Center
Power Plant
Soil Processing Facility
Mass Driver
Science Center
Spaceport
Environmental Operations Center

*Adapted from General Dynamics Space Avionics Requirements Study, Final Task Report, 10/30/90 and Multipath Redundant Avionics Suite Reference Vehicle/Requirements, Preliminary, 6/7/89.

Advanced Avionics
Johnson Space Center

B-92

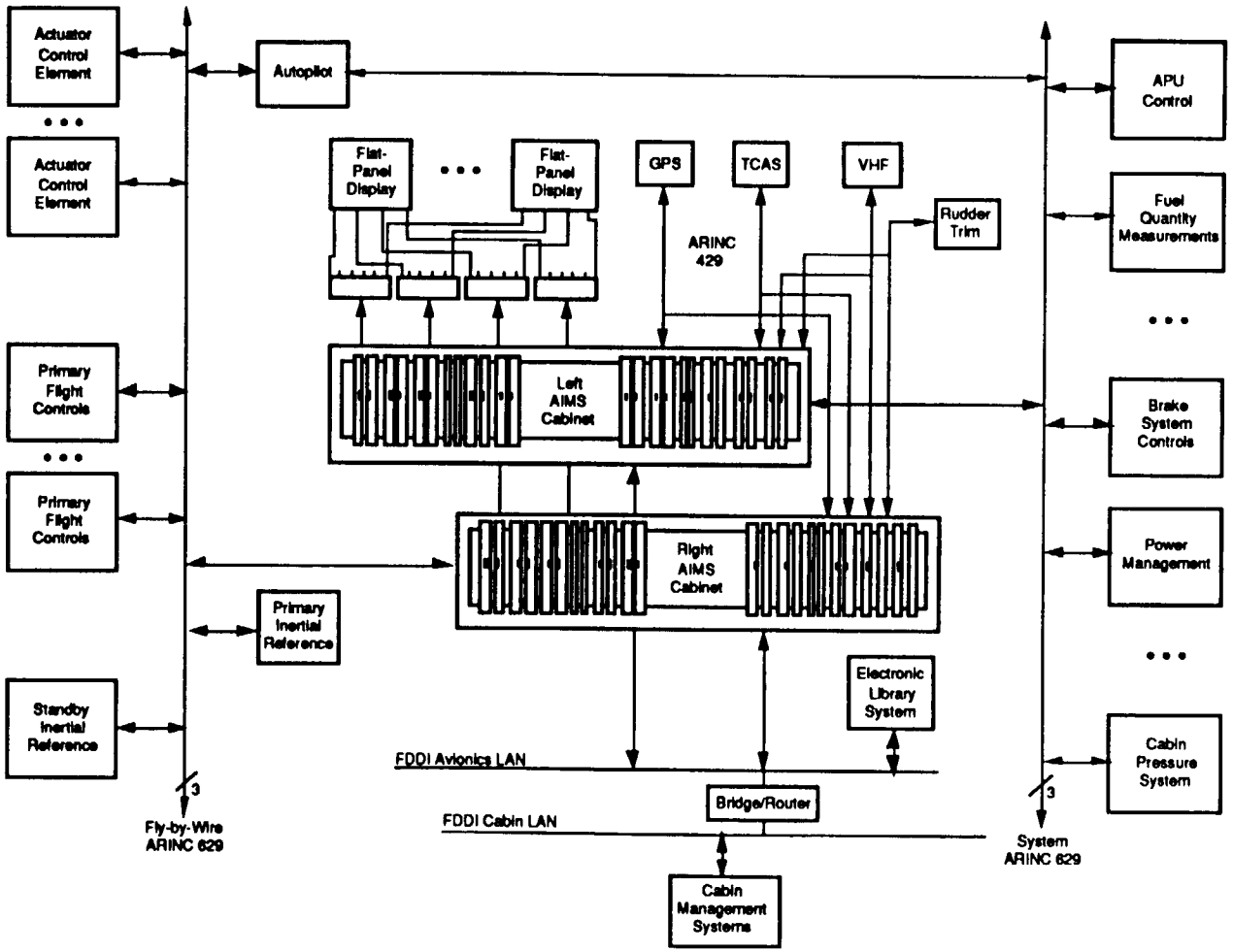
Architectural Configurations

4-4

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

Boeing 777 Aircraft Functional Diagram



Honeywell

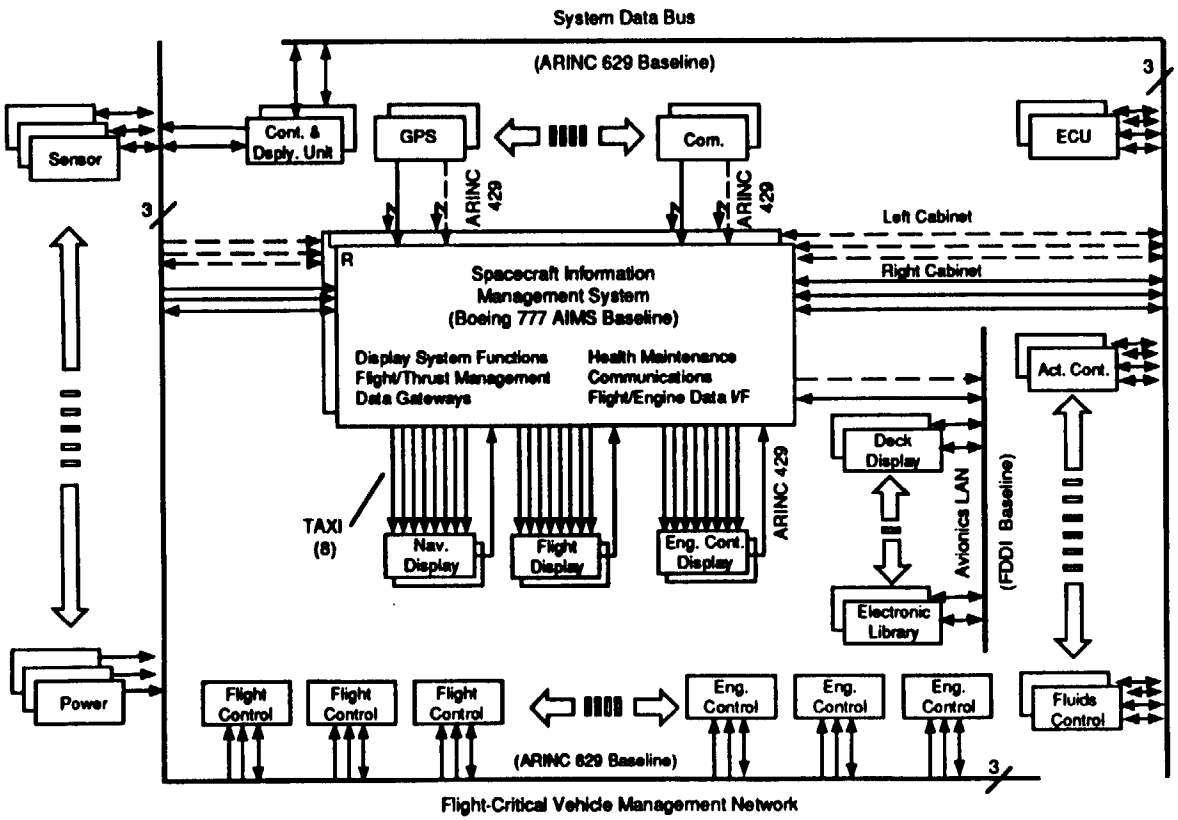
Systems and Research Center

C910929-85

COTS FOR SPACE

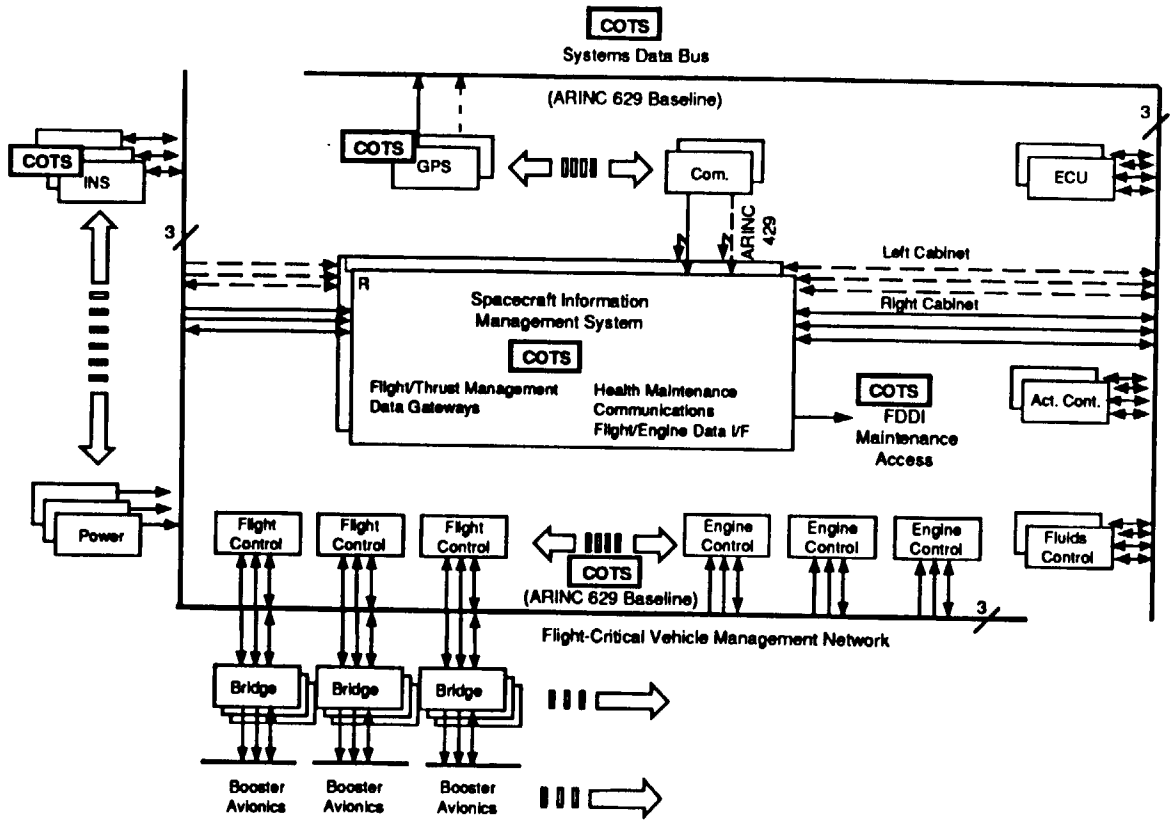
Advanced Avionics
Johnson Space Center

Architectural Framework



- Scalable multinetwork/ bus architecture adapts to different missions/ vehicles and accommodates COTS interfaces
- Point-of-departure design is Boeing 777 architecture
  - Federated hierarchy
  - Distributed processing
  - Flight-critical, fault-tolerant ARINC 629 bus, ARINC 629 system data bus, high-throughput FDDI optical avionics LAN network, TAXI and ARINC 429 bus LRM interfaces

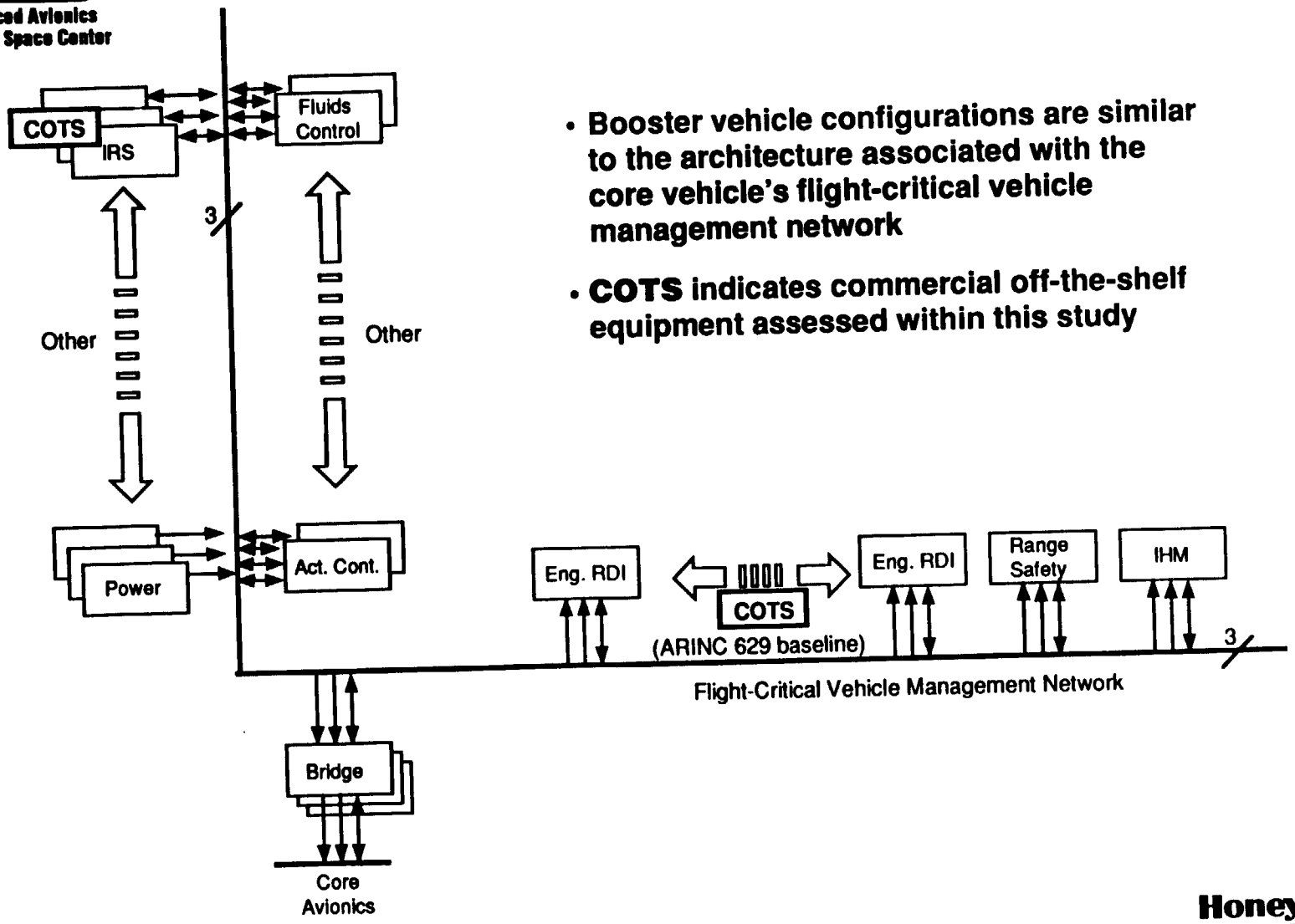
Launch Vehicle Configuration



- Launch vehicle configuration is similar to MPRAS network architecture (Boeing: flight control bus, system bus and transducer network; GDSS: vehicle management network, sensor data network, and test/ maintenance network)
- Alternate connection of GPS or GPS/GLONAS sensor unit to ARINC system data bus is shown
- **COTS** indicates commercial off-the-shelf equipment assessed within this study

Booster Vehicle Configuration

Advanced Avionics
Johnson Space Center

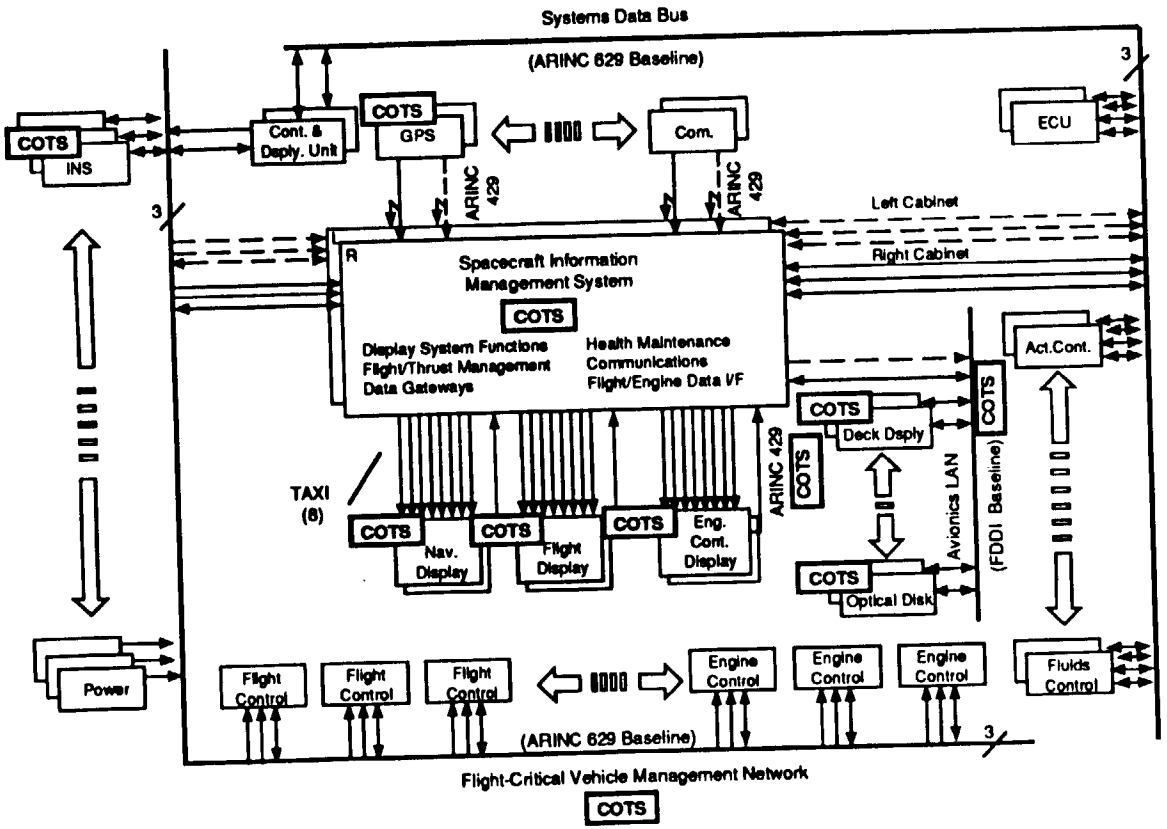


- Booster vehicle configurations are similar to the architecture associated with the core vehicle's flight-critical vehicle management network
- **COTS** indicates commercial off-the-shelf equipment assessed within this study

Honeywell

Lunar Transfer Vehicle Configuration

Advanced Avionics
Johnson Space Center

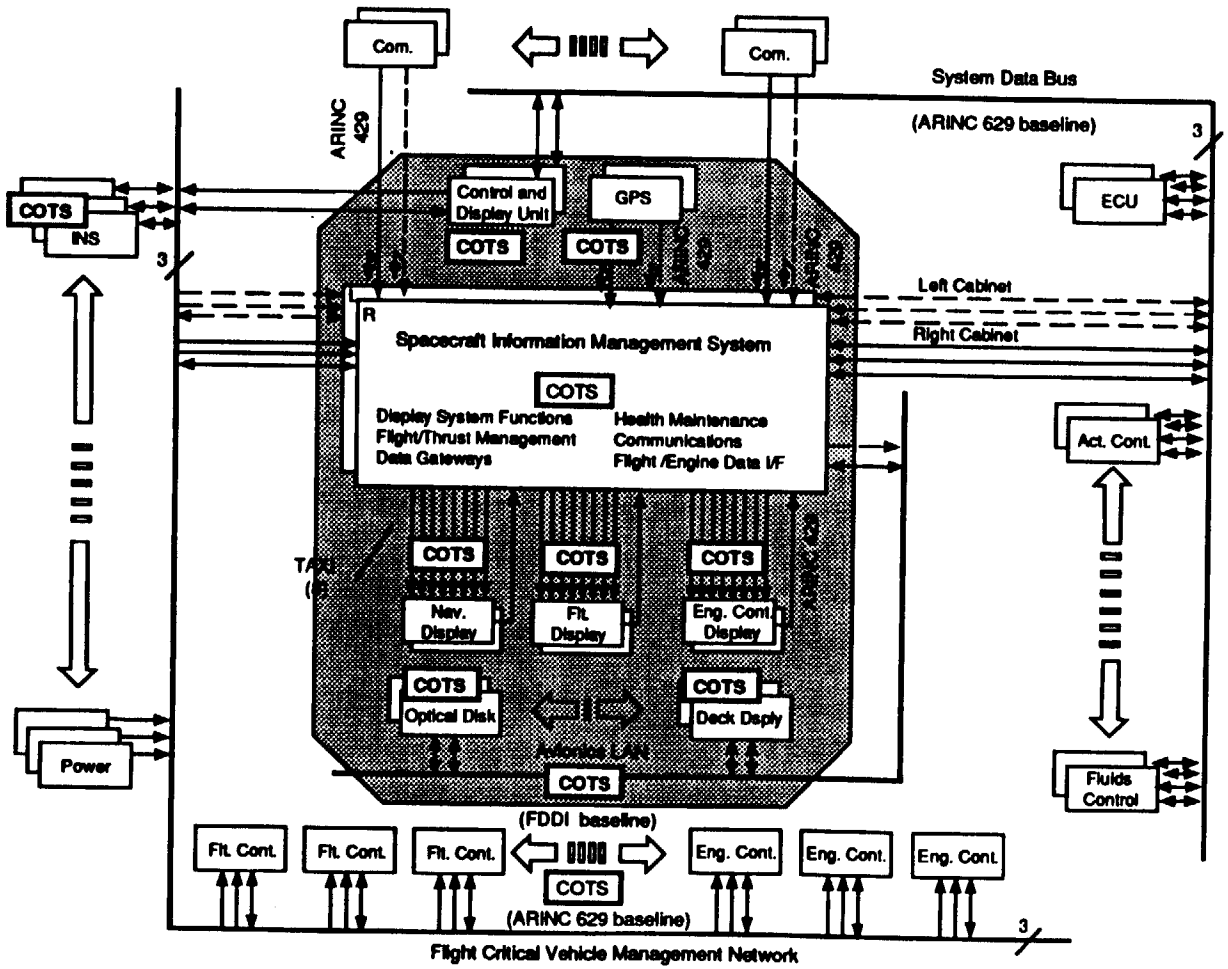


- COTS architecture provides greatest utility for (Lunar and Mars) transfer vehicles
- **COTS** indicates commercial off-the-shelf equipment assessed within this study

COTS FOR SPACE

Advanced Avionics
Johnson Space Center

Transfer Vehicle Partitioning



- COTS [+] components reside in less severe (or controlled), easily accessible environments
- INS products must be able to perform in a variety of locations, must be hard, or vehicle must provide product- compatible environment
- **COTS** indicates COTS [+] commercial off-the-shelf equipment assessed within this study

Advanced Avionics
Johnson Space Center

Summary

Advanced Avionics
Johnson Space Center

PRECEDING PAGE BLANK NOT FILMED

B-103

B-102

Summary of Results

Conclusions

Recommendations

Advanced Avionics
Johnson Space Center

Summary of Results

- A COTS+ avionic system concept was defined and implemented within space avionic architectures

- System specifications, avionic architecture, and COTS+ qualification were modified as required to accommodate COTS+ integration; a relatively small set of COTS+ unique "needs" (or "changes" requiring further development) were identified
  - Distributed, physically partitioned avionics
  - Acceleration qualification as required
  - SEU recovery
  - Humidity and salt spray qualification
  - Acoustic qualification as required
  - Storm cell and safe for cold spares on extended-duration missions
  - Qualification by analysis for outgassing effects
  - Partial vacuum testing as required
  - Configuration and parts control

Advanced Avionics
Johnson Space Center

Summary of Results (continued)

- One concern (a possibly unaccommodating need) was identified—radiation tolerance of commercial parts
  - Possibility of substituting radiation-tolerant parts
  - Using radiation-protected equipment bays or spot shielding

- No technology gaps (development requiring significant involvement, funding, time lapse and/or risk) were identified

- COTS+ reduces space avionic needs and technology gaps
  - COTS+ is available by definition
  - Space avionics requirement study
    - --Red (technology gap) 13 → 7
    - --Yellow (development required) 101 → 41
    - --Green (current/near-term technology) 29 → 95

Advanced Avionics
Johnson Space Center

Conclusions and Recommendations

- COTS provides the space program many attractive benefits
  - Reducing technology gaps
  - Cost-effectiveness
  - Dependability
  - Delivery timelines

- The COTS+ concept for space avionic architectures appears workable in part or in totality. Radiation tolerance of COTS+ products is a concern requiring further assessment. It is recommended that the development needs identified within the study be addressed in ongoing studies. Sponsorship of standards, initiation of technical maturation programs, and further studies are recommended.
  - AHP utility assessments are suggested
  - Deferred maintenance concept should be validated
  - COTS demonstrations are encouraged
  - Transitional integration is suggested
  - A comprehensive development plan is suggested as a next step