DOT/FAA/CT-86/44

FAA TECHNICAL CENTER
Atlantic City International Airport
N.J. 08405

Digital System Bus Integrity

Donald Eldredge
Ellis F. Hitt

Battelle
Columbus Divison
505 King Avenue
Columbus, Ohio 43201

March 1987

U.S Department of Transportation
Federal Aviation Administration

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/CT-86/44		

4. Title and Subtitle	5. Report Date
Digital System Bus Integrity	March 1987
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
Donald Eldredge, Ellis F. Hitt	DOT/FAA/CT-86/44
9. Performing Organization Name and Address	10. Work Unit No.
Lockheed-Georgia Company Marietta, GA 30063	NAS2-11853
	11. Contract or Grant No.
12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Federal Aviation Administration Technical Center Atlantic City Airport, New Jersey 08405	Contractor Report
	14. Sponsoring Agency Code

15. Supplementary Notes

Point of Contact: W. E. Larsen/MS 210-2
Ames Research Center
Moffett Field, CA 94035

16. Abstract

This report summarizes and describes the results of a study of current or emerging multiplex data buses as applicable to digital flight systems, particularly with regard to civil aircraft. Technology for pre-1995 and post-1995 timeframes has been delineated and critiqued relative to the requirements then envisioned. The primary emphasis has been on assured airworthiness of the more prevalent type buses, with attention to attributes such as fault tolerance, environmental susceptibility, and problems under continuing investigation. Additionally, the capacity to certificate systems relying on such buses has been addressed.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
Avionics, Bus Architecture, Bus Topology, Digital Flight Systems, Fault Tolerance, MUX Buses, Networks, Protocols, Requirements, System Integration	Unlimited Subject Category 38

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price*
Unclassified	Unclassified		

*For sale by the National Technical Information Service, Springfield, Virginia 22161

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

DIGITAL SYSTEM BUS INTEGRITY

1.0 INTRODUCTION

Digital buses and microprocessors are used extensively in the current generation of civil aircraft. These buses and processors are used in flight control and avionics applications to transfer data and to perform complex calculations. The Federal Aviation Administration (FAA), at the present time, has no published criteria or procedures for evaluating these complex systems. Currently, the databases and information necessary to develop the regulations, criteria, and procedures required to certificate these systems are not available.

Furthermore, digital systems in the next generations of civil aircraft will require interconnect using digital bus architectures which will be required to have revised interface standards, specifications and architectural considerations in order to provide data to central and remote processors. These digital buses will interconnect microprocessors, sensors, and servomechanisms using diverse network topologies in order to increase their fault tolerant designs and interfaces.

New aircraft incorporating advanced avionic systems/subsystems, will require new concepts in data transfer to accomplish total system integration. The next generation transport aircraft will need total airframe/system integration (on a fulltime/full authority basis) which means new approaches must be developed for the interconnection of avionic subsystems to ensure the integrity of the data at all times. The development of a standard, characterizing a higher order data and information transfer system for interconnecting avionics system, which meets the above requirements, must employ an operational protocol which provides high speed interconnect of subsystems and common sensors, independence, and fault tolerance, as well as distributed control of the common data bus at both the subsystem black box level and the aircraft/mission level.

Future advances in aircraft basic flight control and integration of other avionics subsystems accompanied by a need for total avionics system integration will demand changes in both intra- and inter-subsystem data transfers. These changes, which are due to many factors, include:

- o Need to eliminate costly hardware/software elements required of centralized controlled, data transfer systems.
- o Dispersion of microprocessors within subsystems necessitating the interchange of processed data between subsystems.
- o Need for the generation of an aircraft database, available to all subsystems, which includes all airframe/mission parameters.
- o Maximizing the use of common sensor data and redundant data sources.
- o Making maximum use of multifunctional Control/Display (C/D) elements.
- o Allowance for further standardization of hardware/software elements by use of other standards for interchangeability between the avionic systems and aircraft.

1.1 Definition of Integration Requirements

Present day commercial and transport aircraft employ only single level centralized controlled, command response type or direct-connect undirectional, information transfer systems. The next generation aircraft may have multiple information transfer systems which require interchange of data and will communicate with one another through global memory storage interface units. With systems/subsystems integrated in this manner, a "negative" change in one can result in erroneous data and information being propagated throughout the entire system.

A solution to this potential problem is the development and use of an information transfer system which will efficiently interconnect in a hierarchical order multilevel multiplexed buses and bus architectures. With such an approach, software intensive fault-tolerant executive/operating systems can be created which provide the processing of functions required of multisubsystem inputs within the "local" terminals. Such a high speed higher-order transfer system will probably employ contention or token-passing

protocols which will provide each active unit within the information transfer system structure with the capability of structuring its own functionally isolated communications medium whenever data interchange is required.

The extensive use of existing bus structures has proven the concept of multiplexed data transfer systems to achieve a degree of integration. Unfortunately, current protocols and architectures do not provide the characteristics needed to efficiently operate with the next generations of hierarchical/multilevel networks. The present systems characteristics are ideally matched to many intra-avionics subsystems data transfer requirements which necessitate sensor data collection, central processing, then distribution of results to peripheral areas. There will be and should be continued use of bus networks for the intra-subsystem data transfer.

In the next decade, we can expect some of the more common subsystems to be combined in logical units (boxes) and the emergence of new subsystems or groups of architecturally related functions to be implemented as common units. Each of the major systems/subsystems will also be integrated with each having its own unique intra-multiplexed topological (bus) network. Each of these asynchronous information transfer functions and topological networks must then be interconnected, using high bandwidth buses to create integrated data and management bases from which information flow can be directed and managed.

Such databases, when created, will result in the maximum use of common data and allow for continuing changes in the subsystems and total airframe/mission (flight phase) tasks with minimal disturbance (or perturbation) of the higher-order information transfer functions.

Table 1-1 summarizes the characteristics of the avionics buses in use today, along with the two ETHERNET-type buses currently in use in the computer networking industry. While none of the entries have all the qualities desired for the next generation, the newer network buses offer the greatest potential in light of where the state-of-the-art will be by the time that the next generation of "all new" airframes and avionics are available.

At the present time, data and information for avionics systems integration can be successfully transmitted using these existing or other proposed bus structures. However, each bus has its own limitations which must be considered when assessing the airworthiness of the system.

	ARINC 429	MIL-1553B	ASCB	(DATAC) CSMA CD	TOKEN PASSING
Maximum Bit Rate	100K	1M	667K	10M-20M	10M-20M
Bidirectional	No	Yes	Yes	Yes	Yes
Bus Controllers	No	Yes	Yes	No	No
Defined Data Formats	Yes	No	Yes	Yes	Yes
Low Cost Components	No	No	Yes	Yes / No	No

TABLE 1 SUMMARY OF BUS CHARACTERISTICS

In addition to controlling the flight control and avionics functions of the current and next generation aircraft, the system designers are beginning to incorporate multiplexed "utilities Systems Management" buses in the design of the next generation aircraft. These utility buses will be used to process and send data and information related to Powerplant, Hydraulic, Fuel, Environmental Control, Secondary Power and Electrical Power functions within the aircraft interconnected by redundant buses operating in the 1-10 Mhz range. These utility buses will be operated independently of the Flight Control and Avionics buses; however, they will be controlled by the Master Executive Software resident in one or more Local Area Networks or Token Passing Networks.

2.0 BACKGROUND

The current generation of microprocessor based flight control and avionics systems (as represented by the Boeing 757/767, the Lockheed L1011-500, and the Airbus A310/A320) use bus architectures based on either the ARINC 429-5 or the MIL-STD-1553A/B specification and standards. These buses use shielded-twisted pair wires for the transmission media and interconnect to microprocessors (which primarily use bit slice processors) which provide

the required internal processing speed (7-14 MHz clock rate) and the inherent reliability and flexibility required for flight essential/flight critical control systems. In this generation of digital systems, the individual processors are run in a bit or frame synchronized manner, and the data are exchanged between redundant computers via dedicated serial buses (either wire or fiber optic); and internally by high speed dedicated transfer buses/backplanes.

The next generation of flight control and avionics systems architectures will change dramatically and will be characterized by multiple microprocessors in each computing channel with more local processing within a processor and the transfer of preprocessed data within the bus network. In addition, the system architectures will make use of 16/32 bit microprocessors which will use high speed backplane buses (running at 20-50 MHz) for internal (processor-to-processor) interfaces and exchange of data and information. Furthermore, these processors and their fault-tolerant designs will make use of global memory and functional partitioning of executive and applications software to decrease the complexity and increase the reliability of the system.

Furthermore, the transfer mechanism, as represented by the avionics bus architecture (including the attendant controllers and terminal interfaces) and its transmission media (wire or fiber optic) will play an increasingly more important role in the integration and redundancy management associated with the architecture of the system. The interface circuitry, whether it is implemented using LSI/VLSI chips, or dedicated modules, will be controlled by one or more processor modules and will be implemented in redundant configurations to increase the reliability of the data transfer system.

It is possible, with the ongoing technology developments, to develop a single string physical module which has dual, triple and/or quadruplex path capability and can exist as an integral part of the processor module. This capability, combined with ongoing microprocessor development and advances in internal/external fault-tolerant bus architectures provides the basis for the development of highly integrated, highly redundant, highly survivable computer network architectures in the framework of the digital "all electric" aircraft of the 1985-1995 and 1995-2010 time frames.

3.0 OBJECTIVE AND SCOPE

3.1 Overall Objective

The overall objective of this effort was to conduct an evaluation (through literature search and limited case studies) to determine current and near term Airworthiness/Safety/Structural issues related to the implementation of Digital Bus Architectures in Commercial, Business and General Aviation aircraft in the 1986-1995 and 1995-2010 time frames. The objectives of these evaluations (or case studies) were to provide data and information on the potential airworthiness/safety/structural issues associated with the increased utilization of digital buses in flight control, avionics and utilities architectures in current, retrofit and new design commercial, business and general aviation aircraft of the 1985-1995 time frame; and to extend the FAA's knowledge of the potential airworthiness/safety structural issues associated with the planned implementation of the more advanced architectures in a later time frame. Of special interest, in these studies, was an assessment of the impact of the level of fault-tolerance (including provisions for the effects of electrical disturbances, upsets and interference mechanisms - conducted or radiated) on the integrity of the digital data being generated and transmitted for various bus types and architectures.

3.2 Scope

The emphasis of the study was on the methodologies used to insure the validity of data on buses which use shielded-twisted pair and/or coaxial cable as the data transmission media for data transfer. Fiber Optic cable media is also of interest, especially for the 1995-2010 time frame. Initially, it was not a major consideration for this study, however, due to the recent technological advances and developments in this area, the fiber optic bus/bus characteristics are included in this report.

3.3 Integration Impact

Numerous advantages have been postulated relative to the integration of certain aircraft subsystems (e.g., avionics, flight controls, propulsion, etc.). Such advantages include reduction in crew workload, enhancement of aircraft performance and capability, increased hardware efficiencies and improved flight safety. Examples of integration which provides improved flight safety and reduced pilot workload are autoland systems, flight envelope limiters, and multimode controls.

Traditionally, there has been considerable independence in the design of these subsystems, and components such as sensors were separately provided for each subsystem. However, advanced aircraft designs often require that these systems have significant interaction and have a common data source. The combination of the need to functionally integrate these systems and the desirability of avoiding unnecessary duplication of hardware provides the impetus for developing integration techniques and supporting architectures which both reduce overall costs and increase performance.

Since the avionics and flight and propulsion (as a minimum) are expected to be implemented digitally in current and future aircraft, integration of these systems will probably use one of the buses and/or bus structures, identified in the report, to provide inter-system communication. This method of implementation will allow the necessary sharing of data between subsystems. The desirability to maximize data availability between subsystems is, however, in conflict with the need to isolate these systems from propagation of failures from one system to another. Therefore, the integration solution must consider the balance between the need for and type of integration, versus the flight-safety and mission-criticality of each subsystem as it applies to various architectural implementations within the different aircraft configurations and applications.

The overall advantage of integrating flight-critical subsystems (flight and propulsion controls) with other avionics subsystems can be realized only if efficient, safe and practical methods of subsystems communication can be implemented. Involved in the considerations are architecture topology, design of the bus interfaces, interaction with the host processor (controller) and data bus interface, bus protocol,

hardware/software failure modes, fault propagation potential, and protection mechanisms that prohibit fault introduction or allow detection and management of faults.

4.0 PRELIMINARY ARCHITECTURE CONSIDERATIONS - DATA BUS STRUCTURES

The bus structure for a prototype preliminary architecture (shown in Figure 4-1) is a multilevel concept composed of four (4) digital information transfer bus structures (Sensor, Management, Systems, Actuator) and one or more dedicated analog bus structures. The **Sensor** bus contains data that are time critical and necessary for critical system functions and includes:

- o Body accelerations and angular rates
- o Attitude angle and rates
- o Navigation and position (angles and deviations)
- o Pilot inputs (column, wheel, throttle, etc.)
- o Surface position (deflections and accelerations)

The data handled by the **Management** bus are, for the most part, non-time-critical data that provide control information and system configuration and include:

- o Pilot selected parameters and modes
- o Initialization data
- o Reference angles

The **Systems** bus transfers time-critical data that are provided (by the aircraft avionics and flight controls systems) at a constant update rate to perform mission/flight-phase oriented and automatic functions and include:

- o Auto-throttle position and rates
- o Autoload (deviations, deflections and commands)
- o Attitude reference/control
- o Flight management functions
- o Pneumatic (status/control)
- o Fuel (flow/rate, quantities)

The **Actuator** bus provides the necessary constant update rate data to command and feedback control to the surface controllers and tactile attitude warning devices and includes:

- o Deflection Command/Activator Position (aileron, rudder, elevator, spoiler, stabilizer, etc.)
- o Stability Augmentation (gains/deflections)
- o Stick Shaker

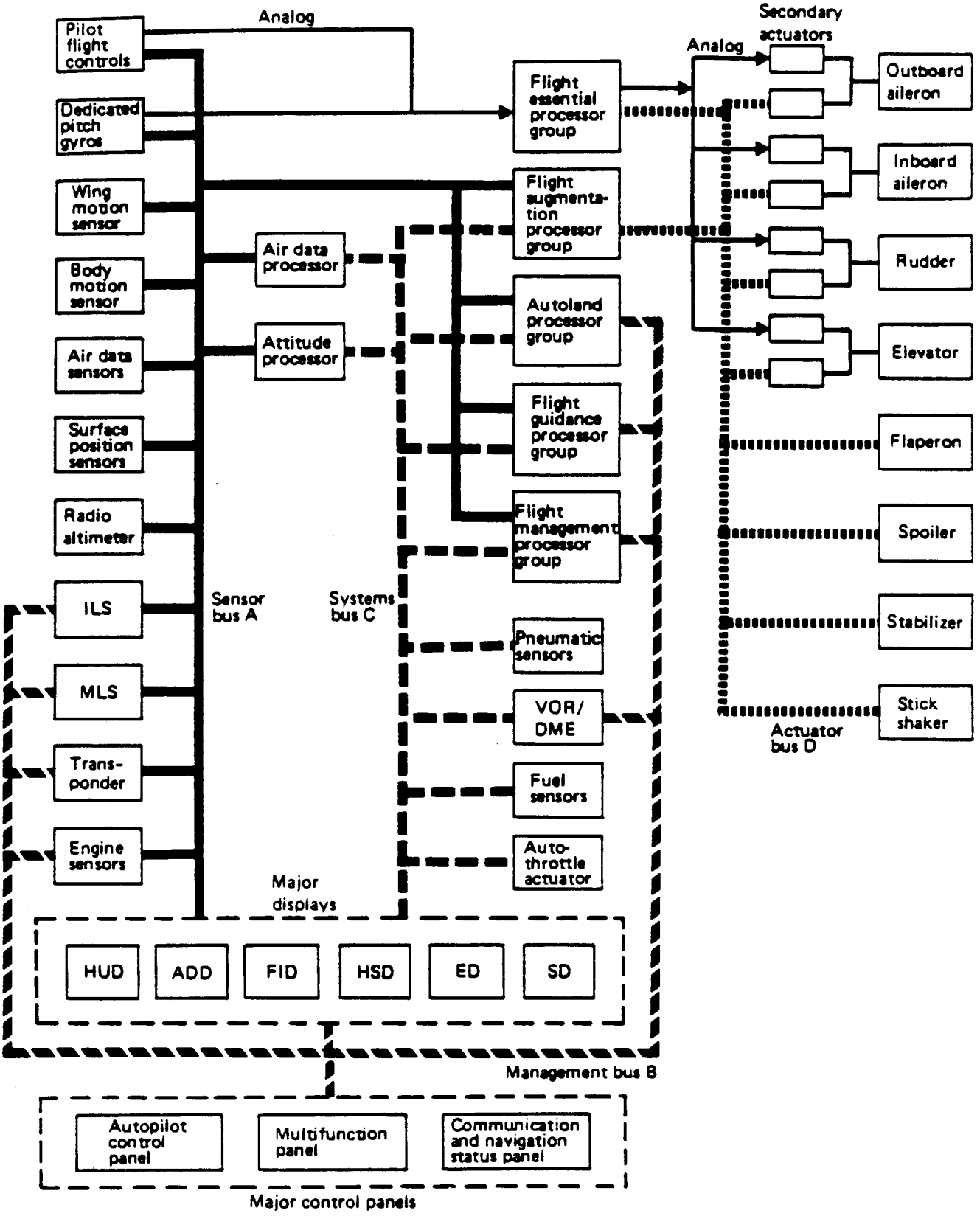


FIGURE 4-1 PRELIMINARY ARCHITECTURE OVERVIEW

The **Analog** (hard-wired) interconnections handle the flight essential functions and include:

- o Pitch rate sensors
- o Pilot flight controls
- o Redundant activators

In general, the prototype multi-level, multi-bus architecture for the next generation commercial aircraft integrates the system functions by data information transfer buses, while separating those functions into smaller functional processing units; and by sharing sensors, decentralization of top-level functional processing covering several computing elements, and by separation of functions by criticality, which results in simplification of system software through greater hardware complexity. Figure 4-2 shows some of the potential bus interconnections that would be implemented for prototype SENSOR, MANAGEMENT, and SYSTEMS buses in the next generation commercial aircraft.

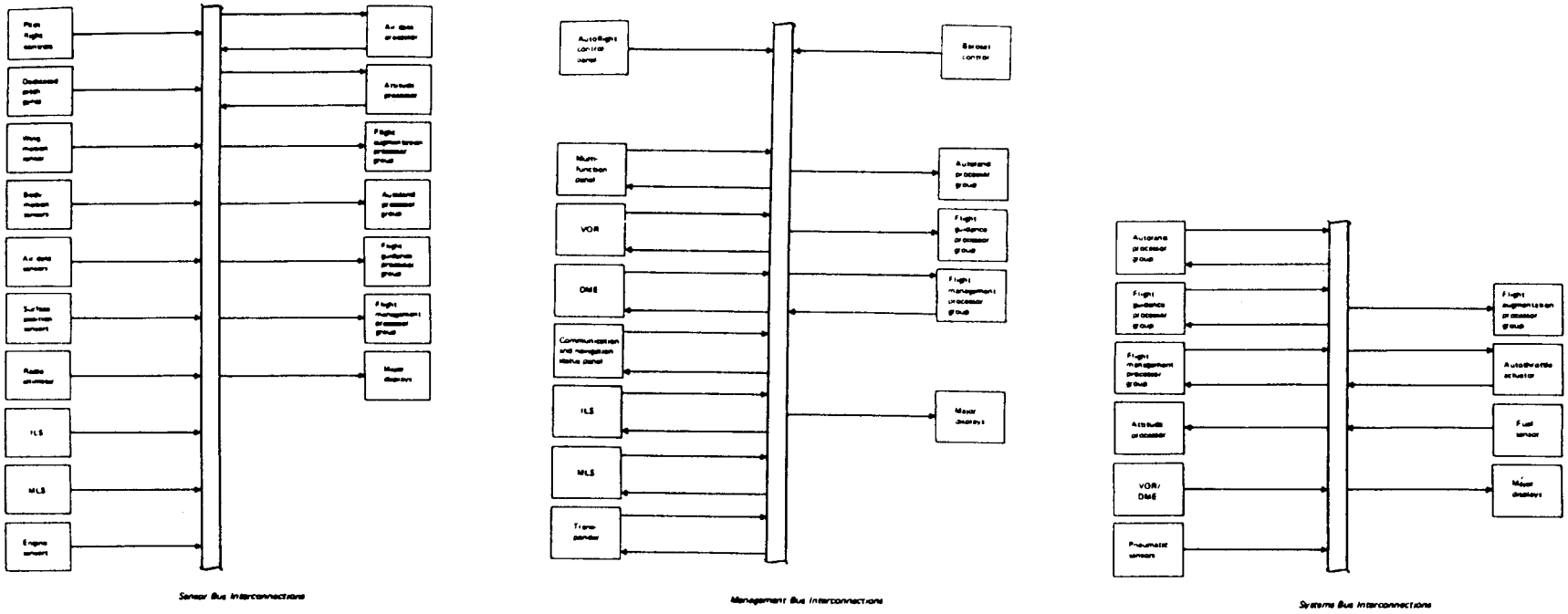


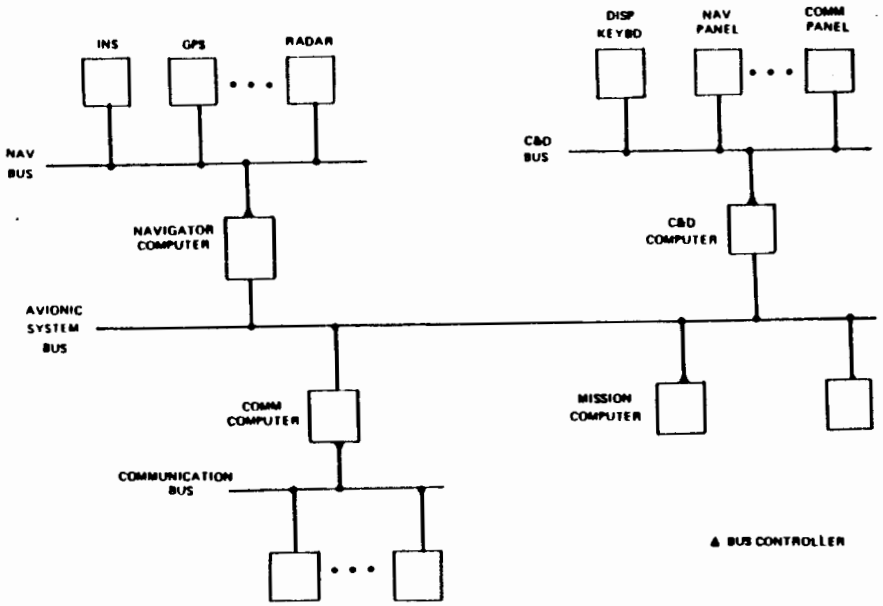
FIGURE 4-2 SENSOR, SYSTEMS, AND MANAGEMENT BUS INTERCONNECTIONS

5.0 TOPOLOGY ALTERNATIVES

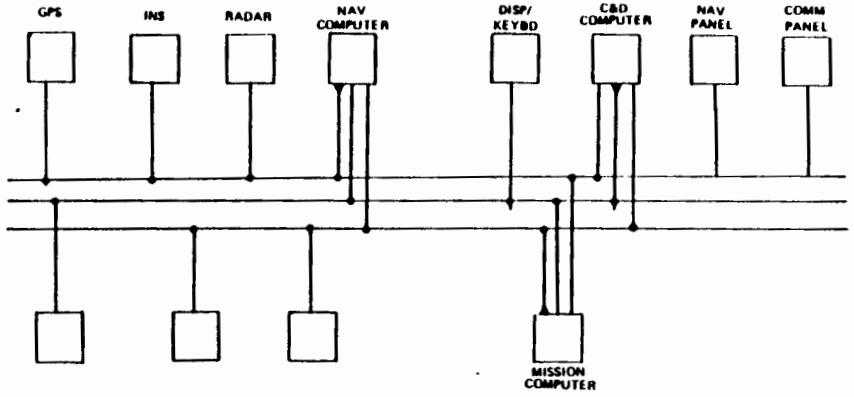
In addition to the prototype architectural considerations discussed above, there exist structural topology alternatives to the implementation of the information transfer buses. Topologically, these buses can be organized as an hierarchical architecture or as parallel architecture as shown in Figure 5-1. In the context of integration with the various avionics and flight control systems/subsystems, different alternatives are available within each of the two bus architectures/structures as shown in Figure 5-2. For example, with the hierarchical avionics bus architecture, the integration can be performed using either a Local Bus or an Avionics System Bus. The parallel avionics bus architecture supports integration over a single bus or multiple buses. Table 5-1 summarizes the advantages/disadvantages of each approach.

Hierarchical Avionics Bus Architecture	Parallel Avionics Bus Architecture
o Local Bus	o Single Bus
o Minimum data latency	o Simpler
o Lowest intersystem impact	o Greater flexibility
o Greater isolation	
o Avionic System Bus	o Multiple Buses
o Information required at more than one local bus	o Higher reliability levels
o Highest inter-/intra-system impact	
o Greater data latencies	

Table 5-1 COMPARISON OF HIERARCHICAL AND PARALLEL AVIONICS BUS ARCHITECTURE

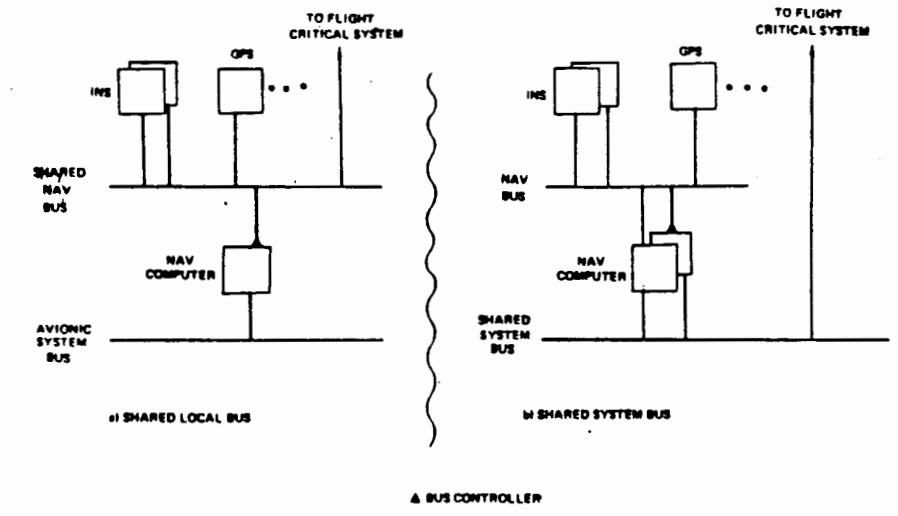


Typical Avionic Hierarchical Architecture

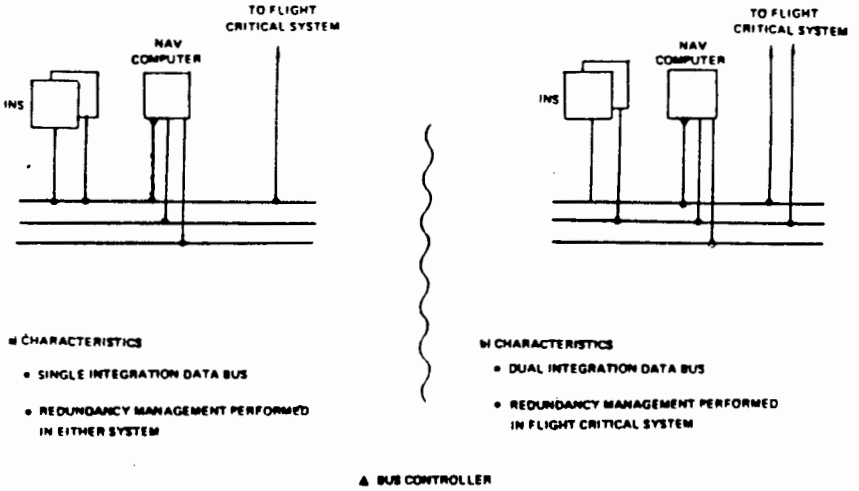


Typical Avionic Parallel Architecture

FIGURE 5-1 TYPICAL AVIONIC HIERARCHICAL AND PARALLEL ARCHITECTURES



Integration Concepts Using Hierarchical Avionics Architecture



Integration Concepts Using Parallel Avionics Architecture

FIGURE 5-2 INTEGRATION CONCEPTS USING PARALLEL AVIONICS ARCHITECTURE

From the control system perspective, three integration alternatives are possible as shown in Figure 5-3. All three cases make use of various combinations of data bus structures (Sensor, Systems, Actuator and Analog) previously referenced, and either use the Flight Control Computers (FCC) as a buffer between the Avionics and Flight Control Systems or connect directly to the control system bus(es) with other mission essential computers acting as the buffer. In either case, the proposed architecture/topology and its attendant integration must be defined in such a manner that either: (a) isolation (in terms of fault propagation) is maximized by integration of functions and sensor signal requirements through the utilization of redundant avionics buses and dedicated buses to support avionics, flight control and other mission dependent functions within the same bus structure (this approach, however, requires higher levels of system/subsystem reliability to satisfy flight safety requirements); or (b) data latency is minimized. By use of separated structures in which critical sensor data co-exists with the flight control and mission dependent computation function on the same bus, and making optional use of existing sensor redundancy with critical sensor data being placed (through multi-party techniques) across the information transfer bus hierarchy, this approach reduces the reliability constraints on each of the various system functions, however, it can introduce new potential failure points into the flight control and mission dependent computation functions due to the increased complexity.

In either case, the selection of a system architecture (including bus structure, topology and integration concept) is based on the design requirements and the preference of the system designer/integrator/implementator. In the concept design phase, a number of candidate architectural concepts, bus architectures, and topologies are postulated, all of which are able to satisfy system requirements within the constraints of the required performance, reliability and safety criteria levels established by the relevant guidance documents (FAR's, Advisory Circulars, and other accepted air worthiness practices). The selection of the final design for the information transfer system will ultimately become a function of selected system/subsystem components, required interfaces, time-critical events/data and the various measures-of-merit attributes that drive the integrator's decisions.

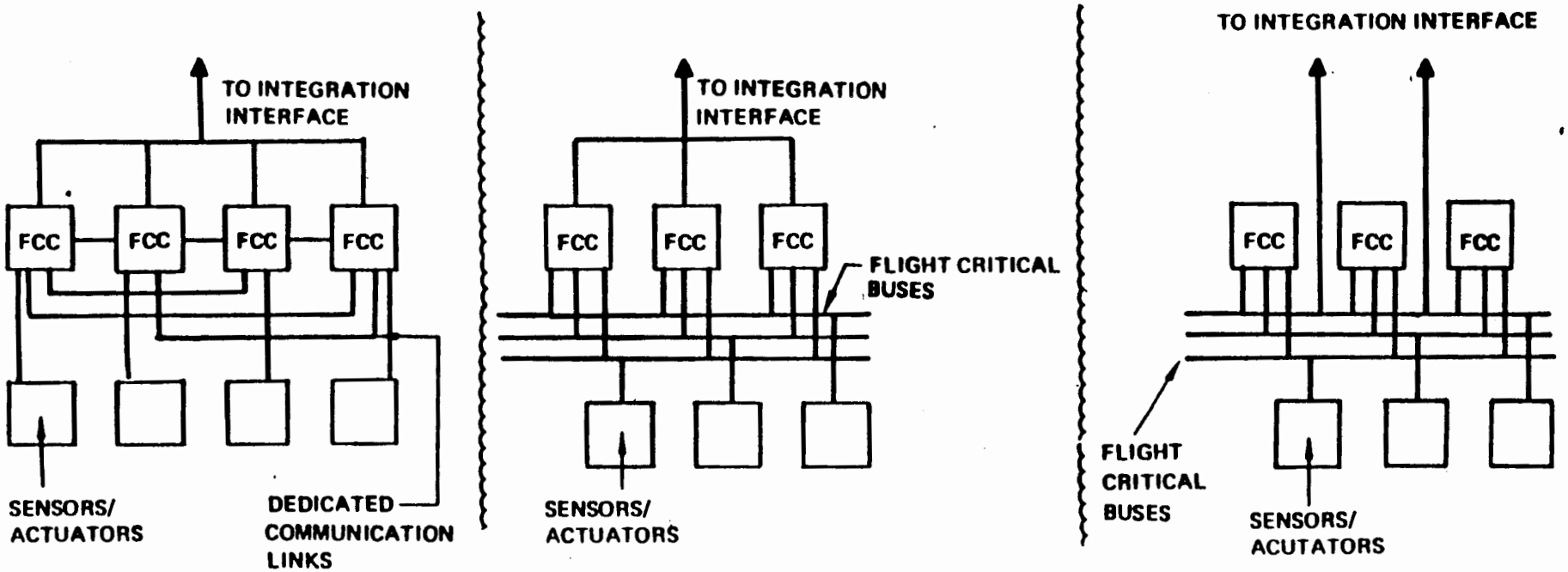


FIGURE 5-3 INTEGRATION CONCEPTS TO FLIGHT CRITICAL SUBSYSTEMS

The measures-of-merit and the attributes (as presented in Tables 5-2 and 5-3) are guidelines to be used by the system designer/integrator to assess the integrity of the proposed information transfer system (its architecture, structure, protocol and integration complexity) and must be considered in order to fully understand and assess the ultimate performance, reliability, safety and air worthiness of the final design.

Table 5-2 presents a summary of the measures of merit and their associated quantitative measures for evaluating a given architecture/structure; and Table 5-3 presents a list of the desirable attributes for information transfer system bus protocols which can be used to quantitatively determine the most advantageous protocol to implement for the envisaged architecture/structure.

Measures-of-Merit	Quantitative Measure
Flight Safety - ability to maintain control of aircraft	Probability of loss of control
Mission/Flight Phase Reliability - ability to satisfy mission requirements	Probability of loss of mission/flight phase capability (i.e., Autoland, etc.)
Maintainability - time required to repair and frequency of repair	Qualitative
Availability - ability to initiate a mission or flight phase activity/ function including full-time, full-authority system (i.e., FADEC, PAS, Envelope Limiting)	Qualitative
Flexibility - ability to accommodate changes	Reconfiguration cost
Reconfigurability - ability to compute or perform mission or flight phase function in presence of failures	Dynamic reconfiguration time or redundancy default (fail safe/fail safe)
Computational Capability - throughput of system computers	Total instructions executed per second
Data Transfer Capability - ability to send messages in a timely manner and in presence of failures	Max data latency, % peak bus loading
Pilot Interface - ability to provide cognitive information to pilot	Qualitative
Cost- initial procurement and Life Cycle Cost	$

Table 5-2 MEASURES-OF-MERIT

Attribute	Quantitative Measure
Fault Tolerance	Probability of error occurring/Reconfiguration time; Probability of propagation
Efficiency	Available bandwidth
Simplicity	Presence/Absence complexity Complexity metric rating
Data Integrity	Probability of connect data transfer Number of retries
Synchronous/Asynchronous	Time to respond to emergency messages/ interruption
Adaptable to new technology Technology Insertion	Qualitative
Similarity to existing bus architectures/ structures/protocols	Qualitative
Deterministic	Qualitative

Table 5-3 ATTRIBUTES

6.0 TOPOLOGIES

In the process of selecting the proper architecture/structure (whatever the application), the following key technology factors (presented in Table 6-1) must be evaluated based on the complexity of system/subsystem being designed/implemented.

- Geographical layout (less than 1,000 meters in range)
- Transmission Topology (linear, ring or other structure)
- Transmission Median (twisted pair wire, coaxial cable (basehand/broadhand), fiber optic)
- Operator type (asynchronous/synchronous)
- Traffic load utilization (burst/regulated)
- Maximum data rate (bits/second)
- Maximum number of nodes (terminals, interfaces)
- Maximum/minimum node-to-node separation
- Maximum number of data channels
- Transmission - delay restrictions (bounded/unbounded, deterministic/probabilistic)
- Access - control scheme (token passing on collision - sense multiple access with either collision avoidance/collision detection)
- Protocols and ISO layers
- Software requirements
- Maintenance, test and error detection/correction
- Safety issues/conditions (EMC/EMI, RFI, shielding and grounding)
- Transaction monitoring, control and testing (single/multiple data-transmitting and/or data-receiving terminals/stations)
- Data, voice, video and/or inquiry operations
- Interactions with other topologies/networks within the same architecture/structure

The technical analyses leading to a selection of a topology/protocol for a given application requires that topologies, protocols, media components, configurations all be analyzed in terms of the system/subsystem constraints imposed upon the detailed system design, and the existing state of technology in each of these areas. In general, a number of topologies and

Fault Tolerance

The capability to endure errors and/or failures without causing total system failure. An important aspect of fault tolerance is recovery, which includes fault detection, fault containment, fault isolation, and reconfiguration. These are defined as follows:

- Fault detection - ability of a system to determine the occurrence of erroneous operation.
- Fault containment - ability of a system to prohibit errors and/or failures from propagating from the course throughout the system.
- Fault isolation - ability of a system to isolate a failure to the required level so as to be able to reconfigure.
- Reconfiguration - ability of a system to rearrange or reconnect the system elements or functions to provide as near the same system level of operation as before a failure.

System Integrity

In essence, the degree to which a system is dependable. System integrity will include the following areas:

- Monitorability - ability of the protocol to be viewed passively to allow observation of the dynamics of the protocol in action.
- Testability - addresses how well the protocol supports completeness of testing and facilitates repeatable or predictable results.
- Initialization - support initial configuration of a system on initial powerup.
- Data Link Assurance of Receipt - support assurance of good data through the data link level.

Table 6-1 CRITERIA DEFINITIONS
(table continues)

Throughput/Response

Measure of how well the protocol transfers data from one node's link level to another. Included in this criteria are the following:

- Effective Link Level Data Throughput - throughput of data from data link level to data link level. It is important to distinguish between actual user data throughput as opposed to percentage utilization or loading of the physical transmission medium.

- Data Latency - time delay through transmission node's data link and physical layers and receiving node's physical and data link layers.

Message Structure

Addresses issues regarding various capabilities and capacities defined by a protocol relative to the structure of the messages the protocol is designed to handle.

- Addressing Capacity - allows system address expansion directly or indirectly.

- Broadcast Capability - allows messages to be transmitted to all terminals simultaneously.

- Block Transfer - mode to allow transfer of variable length data blocks.

- Content or Labeled Addressing - allow terminals to selectively receive messages based on message labels or message identifiers as opposed to "receive" or "destination" terminal addresses.

Table 6-1 CRITERIA DEFINITIONS
(table continues)

Flexible Network Control Strategy

Addresses how well the protocol leaves the system designer free to address his specific problem (design flexibility).

- Central Control - control from one master, whether stationary or non-stationary.
- Distributed Control - concurrent control from multiple points in the data bus system.
- Support of Synchronous Messages - supports transmission of a series of messages at a known a priori sequence and time or time interval.
- Support of Asynchronous Messages - supports allowing nodes on the data bus to transmit a message whose time of transmission is not known a priori. (Also issue of priority messages requiring immediate access to the bus.)

Cost/Complexity

Takes into consideration nonrecurring and recurring cost areas, availability of hardware, firmware, and software from commercial sources as opposed to new development in each of these areas.

- Non-Recurring Hardware and Software Costs - cost and complexity of the design and development of the hardware and software necessary to support the protocol.
- Recurring Hardware and Software Costs - cost of the elements in production needed to implement the bus system.
- Support Costs - cost to support the elements of the bus system once they are in the field.
- Support Costs - cost to support the elements of the bus system once they are in the field.
- Weight, Size and Power - measure of the costs needed to meet the physical requirements of the data bus elements.

Table 6-1 CRITERIA DEFINITIONS
(table continues)

Adaptiveness

Addresses how well the protocol lends itself to flexibility.

- Adaptable to New Technology - how easily can the protocol incorporate new technology.
- Compatible with Old Mechanisms - how well can the protocol support elements which are already in existence for current standards (i.e., hardware, software, control strategies).
- Parameterization Capability - how well can the attributes of the protocol be described by parameterizing those elements which can be so structured.

Table 6-1 CRITERIA DEFINITIONS

protocols currently exist, the most common/applicable to commercial transport implementation are presented in Table 6-2. As can be seen from Table 6-2, the choices for protocols are highly dependent upon the Topologies.

TOPOLOGIES	PROTOCOLS						
	COMMAND RESPONSE	CSMA/CD	TOKEN PASSING	INSERTION ACCESS	TIME SLOT	REQUEST	STORE & FORWARD
Linear Bus	X	X	X		X		
Star	X	X	X		X		
Fully Connected	X	X	X		X		
Ring				X	X	X	
Switched						X	X

Table 6-2 ALTERNATIVE TOPOLOGIES AND PROTOCOLS

Two of the above Topologies have explicit capabilities which are reflected in the planning for the next generation commercial transport information transfer system: The Linear Bus and the Ring Bus architectures/structures. A third possibility, not included in the above, is the currently implemented point-to-point instrumentation of the ARINC 429 Bus structure.

6.1 Review of Protocols

An examination of data bus integrity issues also includes a discussion of the existing bus protocols and their major features. The protocols, in order to insure bus integrity, must be shown to include the following capabilities and characteristics:

- Must be capable of coping with errors
- Must provide the capability of easy retry mechanism(s)
- Must not have failure modes that threaten system failure if an error occurs at a critical point
- Must efficiently utilize the available hardware signalling rate
- Must be free of unnecessary complexity, subtle control issues, and expensive implementation requirements
- Must allow for synchronous, asynchronous or combinations of both operations
- Must not dictate a priority structure for message types
- Must provide data integrity assurance through data transfer confirmation (when necessary)
- Must be adaptable to new technology in terms of transfer media selection, timing and bandwidth
- Must be deterministic with message inquiries being predictable and repeatable

Protocols which meet the above capabilities and characteristics are available for implementation in current and advanced bus architectures, and include:

- Collision Detection -- Boeing DATAC
- Time Slots -- MIL-STD-1553B
- Token Passing -- SAE High Speed Linear/Ring Token Passing Buses

These three protocols are reviewed in detail in the next sections of this report.

6.1.1 Collision Detection

This protocol arises when the transmitting elements of a communications network operate autonomously. There is a probability two or more will attempt transmission at the same time, interfering (colliding) with each others' data transfer.

In its simplest form, this protocol is implemented by letting each terminal transmit whenever it wished. There are, however, a number of inefficiencies associated with this approach. For example, if the data from at least two transmitters is corrupted, it must be repeated in its entirety for all transmitters. Even if a message is quickly repeated successfully the total time to accomplish the transmission could easily be many times the original message length. In addition, there arises the concern for the possibility of repeated collision for a specific message or sets of messages.

Historically, implementations of this protocol have demonstrated that a maximum of less than 20% utilization of the network bandwidth may be attempted before the network stability is threatened. With higher loads, a second collision for a message has a much higher probability. Once this does occur, the total traffic from the first collision, plus that from the second is all thrust down stream in the overall message traffic, increasing the likelihood of additional collisions. In short, at some point the process begins cascading until all terminals in the network become involved and no successful transmissions can be performed.

Refinements of this protocol are numerous. With this protocol, the situation is improved if the second transmitter is smart enough to detect the presence of the first message and delay his own attempt. This approach is known as carrier sense multiple access (CSMA) and when used in conjunction with collision detection is referred to as CSMA/CD which is the technique used in the ETHERNET protocol and is similarly the basis for the DATAC protocol.

With CSMA/CD the occurrence of interfering transmissions is restricted to that situation in which two terminals begin to transmit "so closely together in time" that neither has yet sensed the other's signal. This short time interval at the beginning of a message is referred to as the "collision window" and is simply due to the propagation delay of the network. The collision window is typically on the order of a microsecond in a wired network over short

distances. It can range up to many milliseconds in large networks or even seconds in very complex communications systems.

The improvement obtained by using CSMA/CD is not quite as dramatic as one might expect. While the potential for interference is reduced to the short time of the collision window, a secondary effect of carrier sense is a tendency to synchronize terminals. Since all terminals wait for a quiet network, there is an increased likelihood they will attempt transmissions within the collision window. This thinking suggests the next variation in the protocol. A time interval, called a "mini-slot" is defined to be slightly larger than the collision window. Based on some priority scheme each terminal waits some number of mini-slots following the detection of a quiet network before attempting to transmit. If a higher priority terminal exists in the network it's transmission will begin in an earlier mini-slot and be sensed by the lower priority terminal which will not interfere and simply reschedule its own transmission for a later period of time.

To circumvent these problems, a random selection of mini-slots is used. If a collision is detected the terminal "backs off" a fixed time interval and reselects a mini-slot surrounding the targeted transmission time. Since the terminals operate independently, two terminals which collide once will both back off, select different mini-slots (with high probability) and be collision free in their retransmissions. Should a second collision occur, the terminal doubles its backoff interval and reschedules the message. In general, if n collisions have occurred, the backoff interval is multiplied by 2^n.

The important factor to recognize is that the CSMA/CD protocol is directed at a system of highly autonomous user terminals, a potential drawback to this bus protocol for Avionics Systems interconnect.

Another characteristic of collision detection protocols is that message sequences are necessarily uncontrollable, hence unrepeatable and therefore very difficult to test.

A final consideration relating to collision detection protocols is that the actual collision detection process itself may not be feasible. It was indicated two transmitters would detect each others' transmission and both backoff. But if in fact the signal from the first transmitter is just reaching the second terminal when it begins to transmit, this terminal may quickly detect the collision and abort his own. The result could be a very short

period of interference from the second terminal. This brief signal is attenuated as it returns to the first terminal and there is no clear guarantee that it remains detectable. It is interesting that only ETHERNET anticipates this problem and institutes the jamming pulse train to assure collision detection.

Part of the ETHERNET literature points out another interesting case. Often the carrier sense function is implemented by detecting the phase shift in the waveform. But if multiple transmitter attempt to use the bus simultaneously, it may result in current saturation, holding at a constant level. A saturated bus then looks like an idle bus, effectively inviting other terminals to join the traffic jam.

Collision detection in a fiber optics network is possibly an even more difficult problem. The dynamic range of fiber optic receivers is already an area of concern. The "listen-while talk" requirement of collision detection adds the need to be able to handle the signal from the nearby (it's own) transmitter and yet to be responsive to the distant signal from another unit. It is also conjectured (in some of the literature) that fiber optic receivers that are required to be on while the (necessarily close) transmitters are functioning will have very short lifetimes, significantly impacting maintenance and life cycle costs. (Note: this is the phenomenon that leads to the suggestions of transmissive star couplers, a multi-fiber approach that logically appears to be a bus structure). There exists, therefore, some genuine doubt that a collision detection protocol can readily be transitioned to fiber optic technology.

To summarize then, the analysis of collision detection protocols leads to the conclusions that they require utilization be kept low in order to work well; they may cause significant testing problems due to undetermined, unrepeatable message sequences; and they may not be easily upgraded to new technologies.

6.1.2 Time Slots

A time slot protocol is one in which the use of the transmission medium is pre-allocated. Each of the terminals in the system knows the time it is permitted to transmit and it waits for the time, takes control to transmit (or

receive if the protocol permits this) completes its task and then relinquishes control at the end of its time slot. This protocol approach is also known as time division multiple access (TDMA), or sometimes as "pure TDMA" since the time division is the only basis of control transfer identified in the original statement.

This protocol is strongly synchronous. With a purely synchronous application, all message sequences can be predefined in some optimum fashion. Once a system wide time base is established the terminals can take their turns managing the data flow assigned to them and the control transfer from one terminal to the next can be as rapid as the clock resolution permits. In principle, this protocol can approach 100% bus utilization. Time slotting is highly fault tolerant in the sense that if a potential controller fails, the system continues to operate with the other terminals performing data transfers during their assigned slots. In effect the slot for the failed terminal just goes blank.

The time slot protocol is less fault tolerant when individual message errors are considered. The baseline definition makes no allowance for message retry. If slots are fully assigned and tightly packed (i.e., designed for 100% utilization) the protocol must explicitly prohibit message retry; message errors are basically ignored.

This concern for message retry generates a first variation on the time slot protocol. The slots are oversized relative to the message traffic required in order to reserve a certain fraction of time for message retries. The penalty of course is reduced efficiency. The system designer can elect to reserve enough time to allow all messages to be retried once. He does so however only by driving the efficiency down to a 50% maximum.

In between these two extremes (100% use and 50% use) the system designer may select whatever value is deemed optimum for his system. But now a new concern arises. Once message retries are permitted, but time is not reserved sufficient to retry all, there then exists the possibility of a time slot overrun. To manage this problem, logic (probably software) must be added to make determinations about extending the time slot or truncating message retries in order to stay inside the assign time.

Extending the time slot requires now that the next potential controller (and therefore all controllers) do something like monitor bus traffic prior to

initiating messages. On the other hand, truncating retries in order to maintain the slots leaves the retry strategy less reliable. In short, there is a basic message retry versus efficiency tradeoff to be made and system complexity begins to rise as one moves away from the pure TDMA.

Time slots do not easily accommodate asynchronous message. First, there is the question of allowing time for them. Like message retries, some reserve allocation must be made. And again, either this allocation is very generous (with considerable efficiency impacts) or else the time slot overrun must be dealt with, introducing attendant complications.

Given the above, the response time when providing for asynchronous messages is still not very good; that is, the emergency message is not well handled. It must wait for the next available time slot in order to transmit the message. This problem can be attacked by giving the source terminal frequent short time slots. This, however, is just another way of allocating reserved slot time and it has the same overall system effect.

Another variation on the time slot approach consist of dynamically assigning the time slots. For example the last terminal in a major frame can poll other system elements and plan the next set of slot assignments and broadcast them to other terminals. This approach is much more responsive to a dynamic environment and gives improved handling of emergency message. There is more overhead involved and there are some unpleasant fault tolerance implication. The dynamic slot assignment process becomes a single point of failure and the message communicating the slot assignment becomes a critical message; that is a message that must succeed in order for the system to function correctly.

In summary, the strongly synchronous, very clearly defined time slot approach offers outstanding performance for a highly synchronous system. As deviations from that are accommodated by the protocol, efficiency impacts are accumulated and control complications are introduced fairly rapidly.

6.1.3 Token Passing

This protocol consists of a terminal performing bus control to accomplish its data flow requirements and at the completion of those operations, sending a special message that transfers bus control to another

terminal in the system. This special message contains a data word called a token identifying what terminal is to take control of the bus. The offering terminal at the completion of his operations simply takes the token message as he received it, adds one to the token value and sends out the message.

This elegantly simple control transfer mechanism accomplishes a number of things more or less automatically. First, recognize that when the last terminal to administer control completes its operations a token message is formulated and sent out with a non-existent token number. No terminal takes control, so there is a brief lapse in the data flow. That terminal currently assigned token zero is charged with the responsibility of timing out on this lack of bus activity and starting its own period of bus control. As noted above when those messages are completed, control is then passed to token 1. The protocol automatically restarts itself with token zero regardless of the number of tokens currently active in the system.

A terminal coming on-line to an already active system simply has to monitor the system for a few cycles to see what token message ends each cycle. When no terminal responds to a specific token message, the terminal trying to enter the network appropriates that token number for his own. On the next cycle (or as many as needed to establish the correct token number with some confidence) the terminal responds positively to the token message by initiating his own set of messages and bus control functions. Since this is done promptly, the token zero terminal does not restart the cycle until the new terminal has completed operations, passed on the token, and no other terminal responds to that.

With these defined mechanisms, consider now what happens when a terminal suddenly fails. If part way through a cycle, the token is offered to a terminal that has failed, the token is in effect, "dropped". No terminal takes control and bus activity ceases. When this occurs, the terminal with token zero functions as usual, detecting the lack of his activity and restarting its own period of bus control. The failure of a terminal with a given token causes all higher numbered tokens to be skipped. Logic in these terminals is required to recognize and respond to this situation.

Recognition of this situation is a matter of the terminal timing out on the interval since it last received control. When more than two full cycle times have passed without the terminal receiving the token offer, it decides

something has failed in the network. The response the terminal makes at this point is to decrement its token number by one. On the next cycle the terminal "picks up" the "dropped" token and normal operation of this and higher numbered terminals (which have performed the same process and decremented their own tokens) may now resume. The network response to the failed terminal situation is to run a few abbreviated cycles which effectively confirm the failure and then to close the gap and resume normal operations without the failed unit. When and if the unit recovers, it may attach itself at the end of the loop as previously described.

It is to be noted that the above described mechanism works even for the case of a failure of the token zero terminal. After a period of time, the token one terminal discovers it is not being serviced, decrements its token to zero and assumes the function of starting each cycle. This migration of token number in response to failures implies that all terminals must have the capabilities defined above for the token zero terminal.

The token passing protocol is designed to be highly fault tolerant of controller failures and clearly has achieved that objective.

The approach does not, however, easily satisfy the requirements of a synchronous system. The failure of a terminal in the loop causes the data from that and all higher numbered tokens to simply stop for a while, and then resume operation with a portion of the data flow missing. Subsequent recovery of the terminal may reinstate the missing data but at a different place in the overall cycle. The synchronous system practice of scheduling data flow and task execution with a fixed time relationship would not be reliable.

To try to maintain such a relationship it would be necessary to handle it somewhat like asynchronous tasks. That is, the data arrival could be treated as an event which in turn could be used as a condition for task execution. To accomplish this, software inspection of the data received might be necessary.

Possibly with a careful system design, these problems could be avoided by structuring a strictly receiver oriented message flow. But even then the implication remains that task processing can be reassigned on the time line. This raises a system level issue of whether the designed distribution of processing loads can be maintained.

Neither does the protocol offer a good environment for managing asynchronous operations. Basically, regardless of when the requirement for an asynchronous message may arise, the terminal cannot transmit the message until the token is passed to it. The response time provided asynchronous messages will, in general, average half the total cycle time of the system. But since a terminal can be skipped due to problems with another terminal, not even this time can be guaranteed. A true emergency message, that is an asynchronous message with a very short response time requirement cannot be handled by the protocol. Some add-on such as frequent polling of the source of such messages might be able to achieve the necessary response. Relatively large overhead impacts may be expected in such an approach.

Another area of concern is the impact of errors on the token passing process and vice-versa. It is to be noted that the time out executed by the token zero terminal should be kept small in the interest of efficiency. This time out interval, whatever it is defined to be also defines, necessarily, the maximum time any bus controller may pause during its operations. Should a controller, due to some special situation such as error analysis take too long before its next bus operation there is the possibility that the token zero terminal will interpret this as the end of a cycle and start the next cycle.

When the pausing terminal attempts to resume operations it will now collide with the traffic from the token zero terminal. The normal result of colliding terminals is that both believe they have failed. If this occurs the entire system stops until the other controllers recognize the problem and adjust their tokens. Even at this point the difficulty hasn't been resolved. When the two failed terminals attempt to rejoin the network they will likely collide again. Another possibility, depending on the relative timing in the various terminals, is that one of these recovering terminals could mistake a gap in the network for the end of the cycle. In this case it would appropriate a token already in use and when it attempted to reenter operation it would precipitate the apparent failure of yet a third terminal.

Another potential outcome of the original pair of colliding terminal is that they succeed in establishing apparently normal operations but on separate redundant buses. This eventuality would have less immediate failure impacts but would lead to protracted erratic system operation with the problems occurring at the individual message level.

These kinds of considerations would probably lead to stretching out the defined interval for the token zero time out and require some set of rules for sampling bus activity prior to starting a new cycle. These factors along with some estimates of overall system load would then need to be input to the process of defining the time interval that each terminal would use in deciding when to decrement its token. This would have to be sized for the maximum case and more than likely this time interval would also have to be exaggerated in the interest of caution.

A more pragmatic approach might be to rethink the token passing handshake with a view to making it more ironclad and of detecting a dropped token more quickly. Perhaps for example the message should be "terminal X passing the token to terminal Y with terminal Z selected to validate the handover". A procedure could be developed for terminal X and terminal Z to cooperatively determine when terminal Y had failed. This information could then be communicated to the rest of the system. In general, the more widely distributed the total system state information is, the more reliable the overall operation.

7.0 DATA BUS CHARACTERISTICS

Eight different data buses are either in use or under development for aircraft. Table 7-1 presents characteristics which describe each of these buses.

Transmission Media	Logical Addresses
Characteristic Impedance	Media Access
Main Bus Length	Data Link Control Protocol
Media Connection	Error Detection
Modulation	Synchronization
Signaling Method	Word Size
Transmission Direction	Data Bits/Word
Transmission Method	Words/Message (Min.-Max.)
Transmission Order	Word Types
Data Rate	Intermessage Gap Time
Date Code	Bus Frame Length
Bit Error Rate	Bus Control Transfer Time
Word Error Rate	Terminal Transmit Interface
Topology	Terminal Receive Interface
Number of Terminals/Addresses	

Table 7-1 DATA BUS CHARACTERISTICS

Transmission media include shielded twisted pair wire, coaxial cable, and fiber optic cable. The characteristic impedance of the transmission media is specified by the standard for each data bus. Restrictions on the main bus length are determined by transmission line losses including those due to connection of devices to the bus.

Modulation techniques and signaling method are related to the data code category. Code is broadly categorized as single-density or double-density. Double-density codes include delay modulation (DM), modified-frequency modulation (MFM), group-code recording (GCR), zero modulation (ZM), enhanced nonreturn-to-zero (ENRZ), and randomized nonreturn-to-zero (RNRZ).

Delay modulation, or Miller, coding requires at least one signal transition for every two bit interval and has no more than one transition per

bit, still providing some synchronization capability, at a lower modulation and bandwidth requirement.

The most common single-density codes are non-return to zero (NRZ); NRZ-inverted (NRZ-I), which is sometimes referred to as NRZ-M; NRZ-dual-level (NRZ-L) ratio; and biphase. Biphase covers several subcategories: Manchester II, frequency modulation (FM), and phase encoding (PE). Since these single density codes are self-clocking, the clock is represented by level transitions, which take place even if data transitions do not. NRZ, return-to-zero (RZ), and biphase are categorized by the suffixes L (level), M (mark), and S (space). An -L suffix indicates that data are represented by different levels; -M and -S suffixes indicate that date are represented by the presence or absence of transitions. In codes designated -M, a ONE (defined as a mark) occurs with a level transition; ZERO is no transition. The converse is true for codes designated -S.

NRZ codes remain constant throughout a bit interval and either use absolute values of the signal elements or differential encoding where the polarity of adjacent elements are compared to determine the bit value. This method lacks independent synchronization and error-detection capabilities but provides efficient usage of the bandwidth.

RZ codes return to a binary 0 level at one half the bit interval for binary 1 signals, requiring a higher bandwidth for an equivalent NRZ data rate.

Biphase codes include the Manchester and Differential Manchester techniques. At least one signal transitions is required every bit interval, providing a self-clocking mechanism. The absence of the expected transitions may also be used for error detection. With two possible transitions per bit time, there is a corresponding increase in the bandwidth required.

Multilevel binary encoding schemes use more than two signal levels. One method is bipolar, which has no synchronization capability but does provide some error detection by requiring successive binary '1s' to be of opposite polarity.

Most of the aircraft data buses use biphase codes like Manchester II, which is self clocking since the data and clock are included in a single serial data stream. In clocked systems, the clock defines the size of the data-bit cell; however, in nonself-clocking systems, speed fluctuations cause the data track to vary relative to the speed of the clock. Over a period of time, the

clock will appear to speed up or slow down and improperly define a data bit cell. With self-clocking, everything stays synchronized. The mid-bit transitions of Manchester code help detect transmission errors.

Table 7-2 summarizes the major features for some of the popular single and double-density codes. The encoded waveforms in Figure 7-1 illustrate patterns for an identical binary input produced by each form of encoding.

Code	Bandwidth f_l	Bandwidth f_h	Storage Efficiency	Self-Clocking	DC Presence	Band Speed Ratio	Preamble for Synchronization
NRZ	0	0.5f*	100%	No	Yes	Infinite	No
RZ	0.25f	1.0f	50%	No	Yes	4	Yes
S-NRZ	0	0.5f	80%	No	No	9	No
Ratio	0.75f	1.5f	33%	Yes	No	2	No
Biphase	0.5f	1.0f	100%	No	Yes	2	Yes
Double-density		0.5f	100%	No	Yes	2	Yes

*Bandwidth in terms of the fundamental frequency of the data rate.

Table 7-2 IMPORTANT PARAMETERS OF ENCODING TECHNIQUES

The transmission direction, method, and order define whether data is transmitted and received over the same bus, whether the data transmission is synchronous or asynchronous, and whether the most or least significant bit is transmitted first.

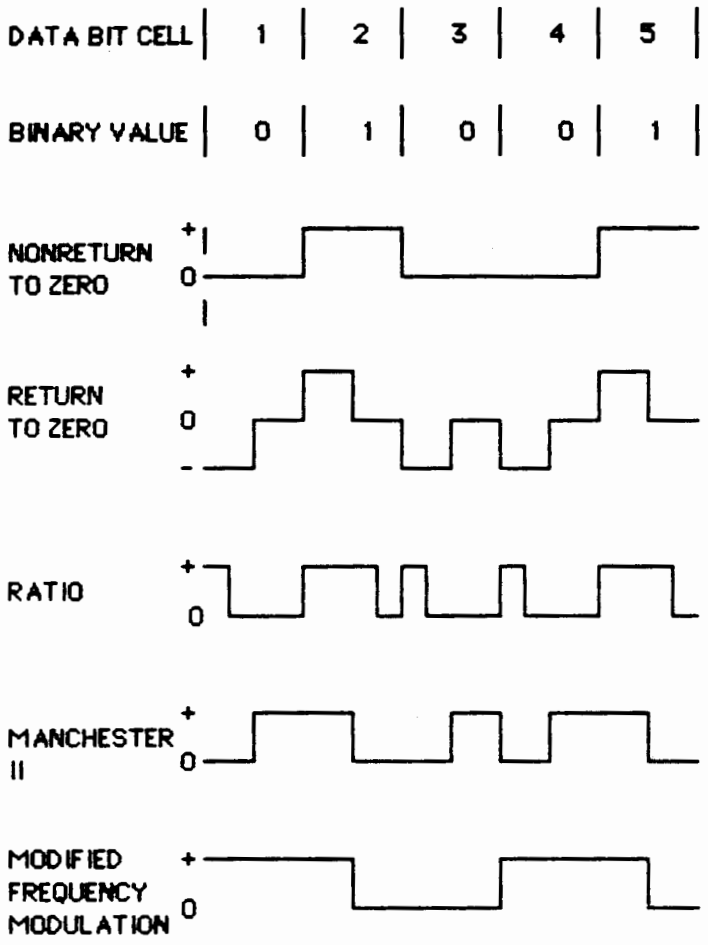


FIGURE 7-1 WAVEFORMS GENERATED BY FIVE DIFFERENT ENCODING SCHEMES FOR A FIXED BINARY SIGNAL

The data rate is the number of bits transmitted per second.

The bit error rate and word error rate are specified values which the bus must meet continuously.

Topology is the architectural configuration of the data bus network. Candidate topologies include the single linear bus (and additional redundant buses), star, ring, tree, near neighbor mesh, completely connected, and the n-cube (n=3) as shown in Figure 7-2.

Additional characteristics include the number of terminals or physical addresses, the number of logical addresses, the method of media access, the data link control protocol, error detection techniques used, and method of synchronization of terminals connected to the physical media.

Two protocols enter into the design of a data bus system. The first is the protocol associated with gaining access to the bus and control of data transmission. The second is the data transmission protocol itself. Both involve certain aspects of fault tolerance including error detection and correction.

One of the control concepts to be considered is the bus access/control transfer protocol. The three basic types are:

(1) dedicated access
(2) polling
(3) random access methodologies.

Dedicated access methods (Space Division Multiplexing (SDM), Frequency Division Multiplexing (FDM), and Time Division Multiplexing (TDM)) permanently allocate each node a portion of the total transmission time.

SDM assumes that a physical line connects each node to a central processor and is virtually contention free. FDM splits the frequency spectrum into channels, which may be statically or dynamically allocated among the nodes. TDM assigns each node a specific time slot during which it has full access to transmit.

The detection of data bus access/control faults is usually embedded in the bus access/control protocol. Watchdog timers and command/response are favored design methods for detection of bus access/control faults. In response to these types of faults, the recovery mechanism usually involves either retransmitting messages, or switching to an alternate controller or redundant data bus.

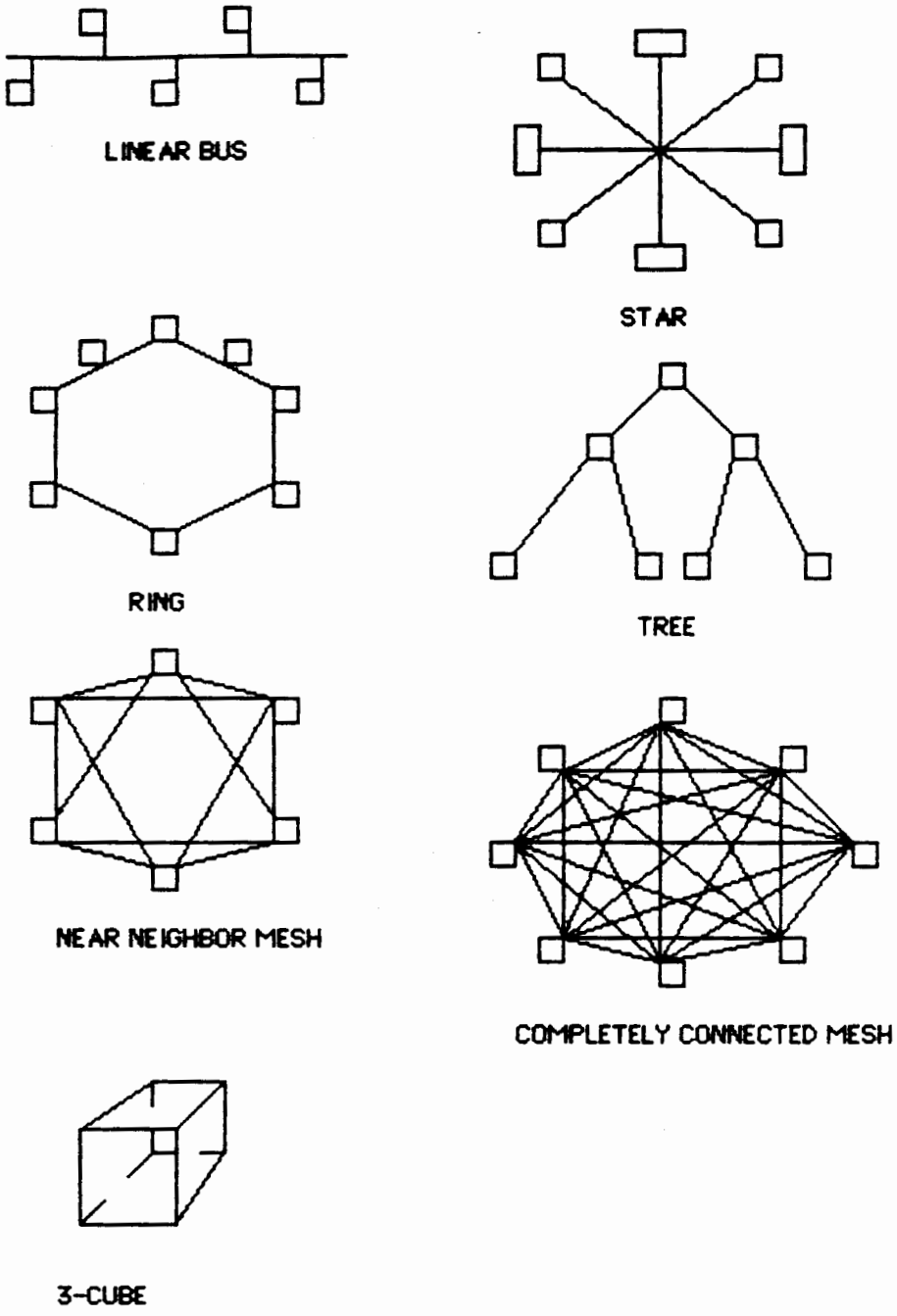


FIGURE 7-2 DATA BUS NETWORK TOPOLOGIES

Data transmission protocols include:

(1) character oriented - Binary Synchronous Communications (BISYNC),

(2) character count - Digital Data Communications Message Protocol (DDCMP), and

(3) bit oriented - Advanced Data Communication Control Procedures (ADCCP), High Level Data Link Control (HLDLC), and Synchronous Data Link Control (SDLC) methods.

The character or byte-oriented protocols use a code set which is shared between both data and control functions; require special escape functions to obtain data transparency; intermix device, message, and link control; perform error checking only on text; and are somewhat rigid in structure.

Bit oriented protocols use specific fields for control purposes, freeing the code set for data (therefore making code naturally transparent); perform error checking on both text and supervisory data; separate link control from device and message control; and are quite flexible and modular.

The protocol must perform the functions of:

(1) initialization - startup of idle communication lines,

(2) framing - determination of transmission block beginnings and endings,

(3) link management - control transmission and reception,

(4) sequence control - avoid duplicates, and request retransmissions for lost or erroneous messages,

(5) flow control - regulate messages transmitted on the media,

(6) transparency - ability to treat all information as pure data, and

(7) abnormal-condition recovery - to treat any illegal commands or conditions.

In evaluating data transmission protocols, the error detection and correction techniques which could be used by the data link layer of the network include vertical redundancy check (VRC), longitudinal redundancy check (LRC), and cyclic redundancy check (CRC). VRC appends one additional overhead bit (a 1 or a 0) to a data word to implement either odd or even parity. VRC does not detect double bit errors. LRC views a frame as a block

of characters, and appends an additional character consisting of the parity bit for each bit position in the character. Even when used with VRC, some patterns of even number errors remain undetected. CRC generates a frame check sequence for a frame which is exactly divisible by some predetermined number which may be checked at both ends of the transmission. Only rare combinations of errors remain undetected with this system.

Forward error correction codes are used when the receiver alone corrects data errors. The codes are calculated and transmitted along with the data. For acceptable correction, data rates are reduced by at least 50%.

Backward error correction (retransmission) is used to resend messages when the receiver signals the transmitter that an error occurred in the transmission.

The number of bits in a word, number of words in a message, word types, and the gap between consecutive messages are important characteristics. Finally, the characteristics of interfaces to the media for transmission and receiving of data are presented.

Characteristics of each bus are presented in Tables 7-3 to 7-10. These characteristics are contained in a single data base which has been broken down into the individual buses for the purpose of presentation in this report.

Table 7-3 presents the characteristics of the MIL-STD-1553 bus.

Transmission Media	Twisted Shielded Pair
Characteristic Impedance	70 to 85 Ohms @ 1 MHz
Main Bus Length	Not Specified
Media Connection	Transformer Coupled
Modulation	Baseband (TDM)
Signaling Method	Biphase Level
Transmission Direction	Bi-Directional Half-Duplex
Transmission Order	MSB First
Data Rate	1 Megabit/Second
Data Code	Manchester II Biphase Level
Bit Error Rate	One Per 10 E12 Bits
Word Error Rate	One Per 10 E7 Words
Topology	Single Serial Bus (Redundant OK)
Number of Terminals/Addresses	31 Addresses - 30 Subaddresses Each
Logical Addresses	Not Specified
Media Access	Command/Response
Data Link Control Protocol	NA
Error Detection	Odd Parity
Synchronization	Word
Word Size	20 Bits
Data Bits/Word	16 Bits
Words/Message (Min.-Max.)	1-32
Word Types	Command, Status, Data
Intermessage Gap Time	4 Microseconds
Bus Frame Length	Not Specified
Bus Control Transfer Time	Not Specified
Terminal Transmit Interface	Not Specified
Terminal Receive Interface	Not Specified

Table 7-3 MIL-STD-1553B DATA BUS CHARACTERISTICS

Table 7-4 presents the characteristic of the MIL-STD-1773 which is the fiber optic counterpart of MIL-STD-1553B. MIL-STD-1773 allows for five possible coupled architectures: reflective star, transmissive star, bidirectional T, unidirectional T, and bidirectional hybrid. The star coupler may be passive or active and can be embedded within the line replaceable unit (LRU) or external to the LRU. Dual speed operation of the MIL-STD-1773 data bus is being examined by a number of vendors to make better use of the bandwidth possible in the bus.

Characteristic	MIL STD 1773
Transmission Media	Fiber Optic
Characteristic Impedance	Not Specified
Main Bus Length	Not Specified
Media Connection	Not Specified
Modulation	Baseband (TDM)
Signaling Method	Biphase Level, 2-State
Transmission Direction	Bi-Directional Half-Duplex
Transmission Method	Asynchronous
Transmission Order	MSB First
Data Rate	Multiple Speed
Data Code	Manchester II Biphase Level
Bit Error Rate	One Per 10 E12 Bits
Word Error Rate	One Per 10 E7 Words
Topology	Single Serial Bus (Redundant OK)
Number of Terminals/Addresses	31 Addresses - 30 Subaddresses Each
Logical Addresses	Not Specified
Media Access	Command/Response
Data Link Control Protocol	NA
Error Detection	Odd Parity
Synchronization	Word
Word Size	20 Bits
Data Bits/Word	16 Bits
Words/Message (Min.-Max.)	1-32
Word Types	Command, Status, Data
Intermessage Gap Time	Not Specified
Bus Frame Length	Not Specified
Bus Control Transfer Time	Not Specified
Terminal Transmit Interface	Not Specified
Terminal Receive Interface	Not Specified

Table 7-4 CHARACTERISTICS OF MIL-STD-1773 DATA BUS

Due to the need for compatibility with MIL-STD-1553B, the MIL-STD-1773 must operate in the time domain and use Manchester II encoding. Matching the Manchester II encoding scheme of MIL-STD-1553B with a fiber optic system results in the average optical power level during each sync code or information bit equaling one-half of the on-power level. Bilevel optical Manchester modulation does have an average optical power of zero when a message is not being transmitted. Consequently, there is a low-frequency component, and it has a fundamental frequency that is equal to the message

rate, often 10 Hz or less. Fiber optic receivers are usually ac-coupled to compensate for the photodetector's electrical signal levels, which are not very large in comparison with the magnitudes of amplified drift and offset voltages. Because of this, special signal processing is needed to offset the effect of the low-frequency component.

Several techniques have been developed for dealing with this low frequency component, but these are susceptible to noise from within the system. The result is the transmitter sections must be much better decoupled from sources of noise in their equipment and must be much quieter when they are not transmitting. In addition, because of the low input power levels to the fiber-optic receivers, the front-end electrical signal levels are much lower in MIL-STD-1773 receivers than in those for MIL-STD-1553B. To obtain satisfactory performance with the greatly reduced signal level, careful shielding is required, as well as decoupling of electrical interference on subsystem lines entering the receiver.

Since optical signals cannot assume negative values, the receiver outputs, which are complementary and thus never low at the same time, cannot be used to identify the no-message state in a MIL-STD-1773 system. As a result, the no-message state and the off state of a two-level Manchester II biphase bit cannot be distinguished. In MIL-STD-1773, it is considered good practice to design fiber-optic receivers with three output states, even though the receivers have only two input states. This is done for compatibility with the outputs of wire-based receivers.

Table 7-5 presents the characteristics of the ARINC 429 data bus.

Transmission Media	Twisted Shielded Pair
Characteristic Impedance	75 ± 5 Ohms
Main Bus Length	Not Specified
Media Connection	Direct Coupled
Modulation	Baseband (TDM)
Signaling Method	RZ Bipolar
Transmission Direction	Uni-Directional
Transmission Method	Asynchronous Broadcast
Transmission Order	LSB First
Data Rate	12-14.5 KHz or 100 KHz
Data Code	RZ Bipolar
Bit Error Rate	Not Specified
Word Error Rate	Not Specified
Topology	Serial Bus
Number of Terminals/Addresses	Less Than 20
Logical Addresses	Not Specified
Media Access	Point to Point
Data Link Control Protocol	NA
Error Detection	Odd Parity
Synchronization	Word
Word Size	32 Bits
Data Bits/Word	19 Bits
Words/Message (Min.-Max.)	1
Word Types	Not Specified
Intermessage Gap Time	4 Bit Times
Bus Frame Length	Not Specified
Bus Control Transfer Time	NA
Terminal Transmit Interface	Not Specified
Terminal Receive Interface	Less Than 20

Table 7-5 ARINC 429 DATA BUS CHARACTERISTICS

Table 7-6 presents the characteristics of the General Aviation Manufacturers' Association (GAMA) Avionics Standard Communication Bus (ASCB).

Transmission Media	Twisted Shielded Pair
Characteristic Impedance	125 Ohms
Main Bus Length	125 Feet
Media Connection	Transformer Coupled
Modulation	Baseband (TDM)
Signaling Method	Biphase Level
Transmission Direction	Bi-Directional Half-Duplex
Transmission Method	Asynchronous
Transmission Order	LSB First
Data Rate	2/3 MHz $\pm$ 0.05%
Data Code	Manchester II Biphase Level
Bit Error Rate	One Per 10 E8 Bits
Word Error Rate	Not Specified
Topology	Dual Serial Bus
Number of Terminals/Addresses	48
Logical Addresses	Not Specified
Media Access	Not Specified
Data Link Control Protocol	HDLC (BOP)
Error Detection	Cyclic Redundancy Check
Synchronization	Frame
Word Size	2 Bytes
Data Bits/Word	16 Bits
Words/Message (Min.-Max.)	1-256
Word Types	Not Specified
Intermessage Gap Time	8 Bit Times (Min.)
Bus Frame Length	25 ms
Bus Control Transfer Time	50 ms
Terminal Transmit Interface	One Bus Only
Terminal Receive Interface	Both Buses

Table 7-6 ASCB DATA BUS CHARACTERISTICS

Table 7-7 lists the characteristics of the Collins Serial Digital Bus (CSDB).

Transmission Media	RS-422A Twisted Shielded Pair
Characteristic Impedance	Not Specified
Main Bus Length	Not Specified
Media Connection	Not Specified
Modulation	Not Specified
Signaling Method	NRZ
Transmission Direction	Bi-Directional Half-Duplex
Transmission Method	Asynchronous
Transmission Order	LSB First
Data Rate	12.5 KBits/Sec or 50 KBits/Sec
Data Code	Not Specified
Bit Error Rate	Not Specified
Word Error Rate	Not Specified
Topology	Not Specified
Number of Terminals/Addresses	Not Specified
Logical Addresses	Not Specified
Media Access	Not Specified
Data Link Control Protocol	Not Specified
Error Detection	Not Specified
Synchronization	Not Specified
Word Size	Not Specified
Data Bits/Word	8 Bits
Words/Message (Min.-Max.)	Not Specified
Word Types	Not Specified
Intermessage Gap Time	Not Specified
Bus Frame Length	50 ms
Bus Control Transfer Time	Not Specified
Terminal Transmit Interface	Not Specified
Terminal Receive Interface	Not Specified

Table 7-7 COLLINS SERIAL DIGITAL BUS CHARACTERISTICS

Table 7-8 presents characteristics of the Boeing DATAC bus. This bus uses carrier sense multiple access with collision avoidance. It provides a complete communication channel from the transmitting system's memory to the receiving systems' memory. Once a terminal has transmitted, it must satisfy three requirements before it can transmit again:

(1) a frame time, common to all terminals on the bus, must have elapsed

(2) a sync gap, common for all terminals, must have existed on the bus

(3) a terminal gap, common for all terminals, must also have existed on the bus.

The receiver of the terminal transmitting monitors the transmission and checks that each label transmitted has been authorized, contains the correct channel information, and the number of words allowed in that string has not been exceeded, and the number of wordstrings in a message has not been exceeded. Any fault causes the transmitter to be inhibited for the remainder of that message. It is allowed to try again on the next frame time. This continues until a certain number of successive tries are unsuccessful, at which time the terminal is permanently disabled. It is not clear how a receiver monitoring fault is handled based on information available at this time.

Transmission Media	Twisted Pair (Non-Shielded, Insulated)
Characteristic Impedance	Not Specified
Main Bus Length	93 Meters
Media Connection	Transformer Coupled (Current Mode)
Modulation	Baseband (TDM)
Signaling Method	Biphase Level
Transmission Direction	Bi-Directional Half-Duplex
Transmission Method	Asynchronous Broadcast
Transmission Order	LSB First
Data Rate	1 Megabit/Second
Data Code	Manchester II Biphase Level
Bit Error Rate	One Per 10 E12 Bits
Word Error Rate	Not Specified
Topology	Single Serial Bus (Redundant OK)
Number of Terminals/Addresses	128 Physical
Logical Addresses	Not Specified
Media Access	Contention
Data Link Control Protocol	CSMA/Collision Avoidance
Error Detection	Odd Parity
Synchronization	Frame
Word Size	32 Bits
Data Bits/Word	16 Bits
Words/Message (Min.-Max.)	1-4096 (256 Words/String, 32 Str/Msg)
Word Types	Not Specified
Intermessage Gap Time	14 Bit Time Min. (Terminal Dependent)
Bus Frame Length	50 ms
Bus Control Transfer Time	Not Specified
Terminal Transmit Interface	Not Specified
Terminal Receive Interface	Not Specified

Table 7-8 BOEING DATAC BUS CHARACTERISTICS

Table 7-9 presents the characteristics of the SAE AE-9B Linear Token Bus.

Transmission Media	Fiber Optic or Electrical
Characteristic Impedance	50 ohms electrical
Main Bus Length	300 m required, 1000 m desired
Media Connection	Optical or Transformer Coupling
Modulation	NRZ
Signaling Method	Biphase Level
Transmission Direction	Bi-Directional Half-Duplex
Transmission Method	Asynchronous Broadcast or Multicast
Transmission Order	LSB First
Data Rate	25, 50, or 100 MBPS (Preset)
Data Code	Manchester
Bit Error Rate	One Per 10 E12 Bits
Word Error Rate	< 1 Every 4 Hours at BIR*
Topology	1 to 4 Serial Linear Buses
Number of Terminals/Addresses	128 Physical - 512 Subaddresses Each
Logical Addresses	2 E15
Media Access	Token Pass
Data Link Control Protocol	Token or Message Frame
Error Detection	CCITT-CRC-16
Synchronization	Frame
Word Size	16 Bits
Data Bits/Word	16 Bits
Words/Message (Min.-Max.)	1-256 Required, 4K Desired
Word Types	Not Specified
Intermessage Gap Time	10 Bit Times
Bus Frame Length	Not Specified
Bus Control Transfer Time	Not Specified
Terminal Transmit Interface	4 Buses
Terminal Receive Interface	4 Buses

*BIR = Benchmark Information Rate

Table 7-9 SAE LINEAR TOKEN BUS CHARACTERISTICS

The AE-9B proposed token passing linear bus protocol involves four simple states:

a) Bus Initialization
b) Normal Token Passing
c) Station Insertion
d) Station Management.

The token is passed from lowest physical address to highest physical address and then back to the lowest.

The worst case delay in the AE-9B linear bus is directly dependent on the maximum allowable message length. Message latency can be easily handled by implementation of system level message priorities.

Table 7-10 gives characteristics of the SAE High Speed Ring Bus (HSRB).

Transmission Media	50 Mbps Coax, 100 Mbps Fiber Optic
Characteristic Impedance	75 ohm Triax
Main Bus Length	2 km Ring Length
Media Connection	Optical or Transformer Coupling
Modulation	NRZI
Signaling Method	Biphase Level
Transmission Direction	Uni-Directional
Transmission Method	Asynchronous Broadcast
Transmission Order	LSB First
Data Rate	10-1000 MBPS
Data Code	
Bit Error Rate	One Per 10 E12 Bits
Word Error Rate	Not Specified
Topology	Ring - 2 to 128 Stations
Number of Terminals/Addresses	128 Physical - 512 Subaddresses Each
Logical Addresses	2 E15 - Broadcast and Multicast
Media Access	Token Pass
Data Link Control Protocol	Token or Message Frame
Error Detection	CCITT-CRC-16
Synchronization	Frame
Word Size	16 Bits
Data Bits/Word	16 Bits
Words/Message (Min.-Max.)	1-4096
Word Types	Not Specified
Intermessage Gap Time	Not Specified
Bus Frame Length	80K Bits
Bus Control Transfer Time	10 Million Data Bits
Terminal Transmit Interface	4 Buses
Terminal Receive Interface	4 Buses

Table 7-10 SAE HIGH SPEED RING BUS CHARACTERISTICS

The ring bus offers superior throughput capability when compared with the linear bus due to short point-to-point media links between nodes. In the area of fault recovery and reliability, the ring is less attractive due to the need for failed node bypassing using either mechanical relays or fiber optic switches. Ring reconfiguration may take up to 25 msec when bypasses are activated. In addition, a limit must be placed on the number of consecutive nodes which may be bypassed, due to a lower power budget in the

short point-to-point links and the relatively high losses inherent in the bypass devices (both wire and fiber optic).

8.0 BUS PERFORMANCE CHARACTERISTICS

The performance characteristics of a bus, in a given architecture, are affected primarily by Data Latency and System Delays.

Data Latency

Data latency is the delay from the time when a piece of information becomes available at a source terminal to the time it is received at the destination. The degree of latency is affected mainly by the architecture and the protocol of the message transmission. Hierarchical architectures, as previously defined in Figure 5-1, are inherently subject to longer delays than are parallel architectures, due to the number of nodes (common exchange points) through which a message must pass. When an hierarchical interface is used, and time sensitive information is transmitted between levels of the hierarchy, time tagging of the data messages may be necessary. The time tag (if implemented) would become part of the message and would be used at the destination to determine the "freshness" and/or urgency of the message/data. In the case of an hierarchical architecture, such as that in Figure 5-1, node information is made available at different times at various levels of the architecture, dependent on the number of nodes through which it must pass. For example, if the flight control computers control the initial transfer of the node data/status, and depending upon the protocol, the node data/status information can then be made available to mission oriented computers and/or other FCC's with minimum delay. The next level transfer is controlled by the mission oriented computers, and again depending upon the protocol, the data/information will eventually (after incurring routine delays) arrive at the destination terminal/computer, and eventually the end destination (in this example, the video display or graphics generator computer). During this same period, the applications computer (avionics, navigation, etc.) can be providing information to other computers, within the hierarchical architecture, based upon the node data/status information it currently has available. If however, the node data/status information had been changed during an activity controlled by the other applications computers, there is a potential for error introduction due to one or more of the flight control computers being in a node status different than the other avionics or flight

control computer currently performing the activity. In order to minimize the potential for error due to latency, the node data/status message could include a time tag generated when it is/was sent from the node select computer. When each successively higher level within the architectural hierarchy generates a message/command, it would automatically pass along the time tag of the node data/status message. When the message arrived at the various destinations, within the hierarchy, a comparison would be made of the current and new node data/status values and the time tag to ascertain the validity of the command. In general, the actual latency of a message within a given architecture is determined by the rate at which the bus structure (either autonomously or centrally controlled) allows a "sending" terminal the opportunity to "latch-on" to the bus in order to transmit its message/data. For a centrally controlled bus, to obtain the least possible (i.e., minimum) latency, the bus controlled would be configured to (a) continually poll the terminals within the bus structure, (b) sense (respond to) the service request bit in the terminal status word, and (c) initiate the terminal-to-terminal (or terminal-controller) message transfer.

With an increase in the distribution of processing tasks to more specialized computers and away from a central general purpose computer concept, an event based scheduling scheme may become a good alternative for some applications. When task scheduling is based upon events rather than time, the latency of a message becomes more critical and the continuous polling technique is an effective way to reduce the message latency. For an illustration of the event based scheduling, refer to the local display bus of Figure 8-1. The display computer is normally operating in response to messages from the mission computer, and its BCIU which controls the local display bus is continuously polling for keypad entry. When the keypad is pressed a message is sent back to the display computer, signaling an event to which the display computer must respond. The display computer will break out of its normal cycle, process the keypad message, and upon completion of this processing will have available keypad information that can be sent to other devices on the mission computer bus.

In this application two advantages are obtained from the event based scheduling and continuous polling. The latency of the message as it passes from a local bus to a higher level bus is minimized, and component faults in

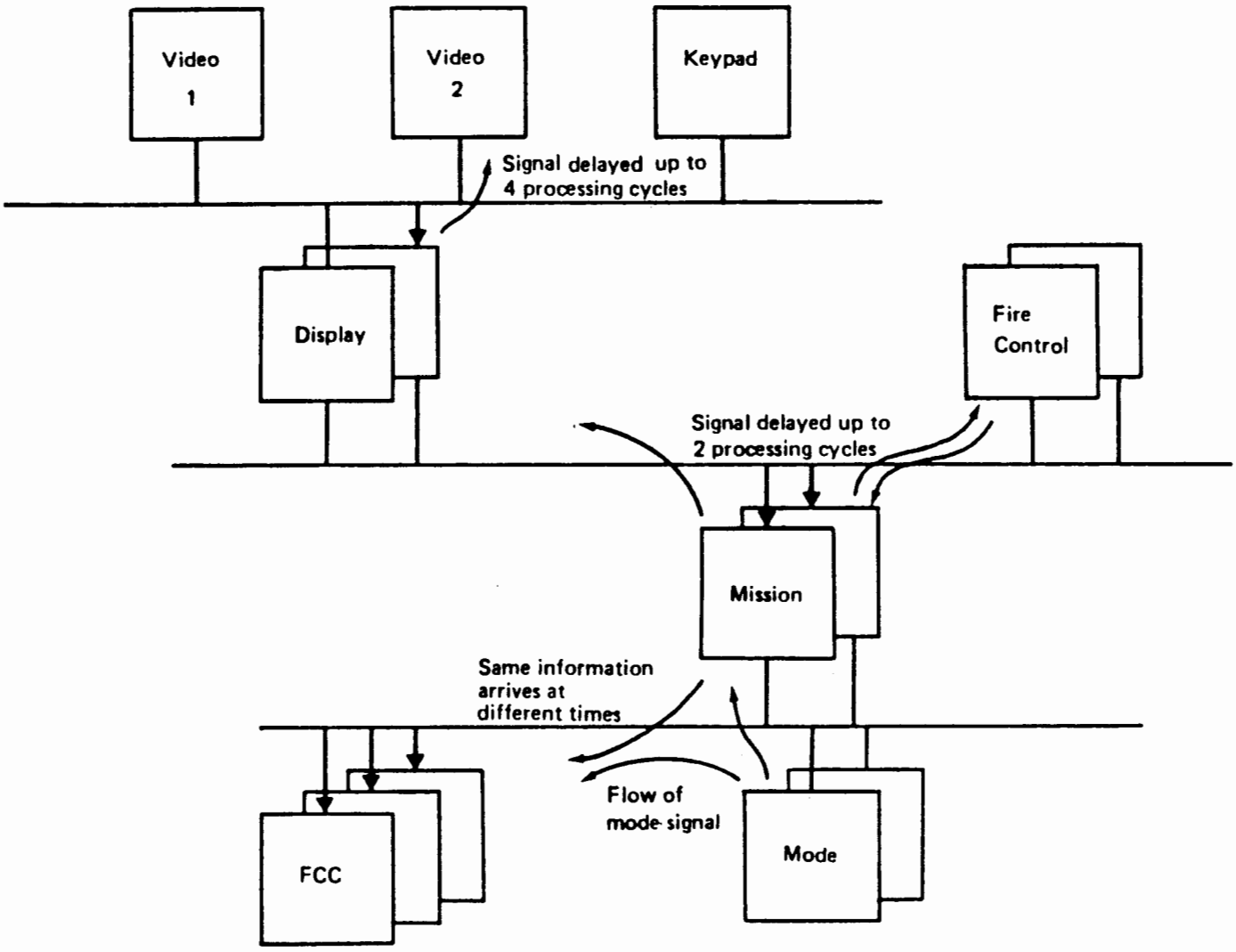


FIGURE 8-1 DATA LATENCY ILLUSTRATION IN HIERARCHICAL ARCHITECTURE

the communication system are identified early to provide time for management of the failure. For example, a simple management scheme would be to retransmit if the status response were not returned with the message error bits clear. On the negative side, the checkout is more difficult due to the inability to repeat a particular condition. When all scheduling is time based, then a repeatable test scenario can be generated and system response evaluated deterministically. When operation is based on asynchronous events, only a statistical comparison of results from multiple tests is valid.

On a single hierarchical level there are several protocols than can be used within the bus architecture framework, and this protocol choice affects message latency. The use of a stationary master that polls all terminals on a regular basis provides minimum latency for a small number of terminals on the bus. A second approach where bus control is exchanged among a limited set of master computers introduces potentially greater latency, depending upon the message table orientation of each master computer. If bus control capability exists in every terminal that may have a time critical message, the message latency will be in the range of several (2-4) milliseconds. If continuous polling is done between every message transmission, latency improves; however, a large bandwidth penalty is paid. Continuous polling can only be used on buses with low activity levels.

System Delays

Average transfer delay is defined as the sum of delays resulting from queueing delay, access delay, and transport delay.

Queueing Delay. Queueing delay is characterized by message arrivals and arrival rate and represented (characterized) as a Poisson Distribution. The mean queueing delay consists of the average delay incurred due to a message waiting for a previous message within the BIU to be serviced. The BIU's are effectively a single server queue, and therefore the queueing delay is a delay imposed on the user due to the BIU transmit buffer being full. This delay neglects the user/BIU interface message processing rate limitations and is dependent only on the message interarrival time as determined from the offered load.

Access Delay. In the case of the CSMA/CP protocol, the mean access delay is determined by considering the two inherent access modes. The delay due to the random mode and the delay due to the ordered access mode are

factored with the probabilities of being in their respective states and combined to equal the mean access delay.

For the random access delay there are two components of delay: 1) delay due to the bus being busy, and 2) delay due to a collision. For the bus to appear busy, at least one other message must arrive before the message that encounters the media active state. Therefore, the probability of the bus being busy is the probability of two or more arrivals within the same time window.

The probability of a collision can be described by the probability of two arrivals in time and the probability of three or more arrivals in time. The delay due to a collision is determined by the time required to recognize a contention, issue the jamming signal (approximately 1 microsecond), wait for the appropriate gap time, and then the wait until the appropriate time slot. Because the load distribution is assumed to be equal among the network BIUs, the average delay for the time slot count to reach the assigned time is one-half the total scan time for the time slot sequence as determined by the loading conditions.

Looking at the access delay encountered by a message arrival during the ordered access mode, two conditions are possible: 1) message ready before the time slot arrives, or 2) message ready after the appropriate time slot has passed. For an equal load distribution, the probability of each case is 0.5.

Transport Delay. The transport service time is determined by the transmission rate, the message length, and the overhead required for each transmitted packet. The overhead includes the following:

- T_{gap} between messages
- Turn on time (power strobed BIUs)
- Packet encapsulation
- Propagation delay of 50 meters
- Acknowledge turn on plus
- Propagation delay
- Acknowledge message

System level fault management is further facilitated by the monitoring of network statistics at each node. During operation, the BIUs collect the following statistics:

- Number of collisions
- Number of collisions during own transmission
- Number of packet rejects due to decoder buffer full
- Number of successful transmissions
- Number of unsuccessful transmissions
- Number of data transmissions received
- Number of status responses received
- Number of commands received

9.0 FAILURE MODES AND EFFECTS (BUS ARCHITECTURES)

Operation of the current and next generation digital aircraft requires the proper function of a number of interrelated/interconnected systems/subsystems/components within the framework of an integrated bus hierarchy/structure. Intermittent or erratic behavior or total failure of one or more modules/components can impact the ability of the aircraft to perform its intended function. In some cases, the impact will be transparent as the fault/error/mistake is automatically detected, the failed module/component identified and a redundant "like element" (similar or dissimilar) activated or "switched-to" automatically. Continued successive failures (or in the worst case, multiple simultaneous failures) could result in increased pilot workload, loss of function, or in the most severe case, the total loss of aircraft.

Because of the nature of the interactive relationships of systems/subsystems in these aircraft, failed modules/components may affect not only the subsystem in which they are embedded, but the failure's effects may propagate into other subsystems. This failure propagation potential between multiple systems/subsystems is greatly magnified by the differing levels of "functional integration" where data and information are exchanged between and among systems/subsystems (using bus architectures and structures) as a requirement for normal operation.

Failures that could cause loss of essential mission capability or loss of aircraft must be protected against by using equipment redundancy, analytical redundancy, or "functional redundancy" to provide for continued operation after one or more failures. The redundancy may be applied at the system level (multiple buses or flight control computers), at the sensor level (redundant INS, AHRS, DADC, etc.), or at the module/component level (multiple similar or dissimilar microprocessors located in multiple processor subsystems). Failures that result only in some loss of function, restricted operation, or increased pilot workload, may or may not require redundancy, depending on the exact nature of the loss and the probability that such a loss will impact aircraft performance capability (i.e., navigation or position location) or aircraft flight safety (i.e., CAT II or CAT III landing). Failures that reduce the level of hardware redundancy or

analytical redundancy, without loss of functional capability, may be able to be tolerated without performance degradation.

Failures can also result from external disturbances or internal malfunction and can be either transient or permanent. Transient faults can often be ignored if the system is designed to tolerate such faults. In other cases, a transient fault can cause a more serious failure, such as the interruption of an instruction sequence in a computer, which in turn could cause a time-out or retry sequence, resulting in the completion of the computation using "stale" data. Permanent failures, on the other hand, must be recognized as such, and action taken to reconfigure around the failure.

Environmental effects can often be the cause of the failure. In the case of wire buses, heat, power supply surges (spikes), or low voltage levels could cause permanent or intermittent operation of an electronics unit or corruption of the bus data, which in turn would cause incorrect data and/or information to be passed to another unit in the hierarchy. Loss of electrical integrity (due to faulty shielding, grounding, or loss of cable integrity) could result in susceptibility to electromagnetic radiation, thus causing erroneous or erratic behavior.

In general, failures may exist in any one of the five functional elements relating to the integration of two or more subsystems. These functional elements include:

(a) computers which process the data that are exchanged between subsystems;
(b) the data bus interfaces;
(c) the data bus(es) themselves;
(d) the input/output devices that govern the transmit/receive functions; and
(e) the system errors.

Table 9-1 summarizes the potential faults which can cause intermittent or erratic behavior or even total failure of the networked architecture to communicate data and information to the various systems/subsystems within the structure.

1.0 COMPUTER FAULTS	2.0 DATA BUS AND INTERFACE	3.0 INPUT/OUTPUT	4.0 SYSTEM REDUNDANCY/MANAGEMENT FAILURES
1.1 Computer Hardware Faults	2.1 Data Bus Hardware	3.1 Input/Output Device	4.1 Design Failure (Fault)
1.1.1 Central Processor Unit (CPU) Failure	2.1.1 Open/Short-Single Bus/Multiple Buses	3.1.1 Hardware Failures	4.1.1 Synchronization-Time Skews (Comparison Monitoring of Time Tag Data)
1.1.2 Memory Failure (Error)	2.1.2 Interface Unit Failure	3.1.1.1 Sensor, Sensor Output Transducer, Discrete Signal Input Failure	4.1.2 Generic Failure Modes - Power Interrupts, Software Design Faults, Common Mode Failures
1.1.3 Discrete and Analog Input/Output Failure	2.1.2.1 Failure to Respond	3.1.1.2 Induction of Noise (or Other Oscillary Disturbance) Due to EMI/EMC	
1.1.4 Clock Failure	2.1.2.2 Response to Wrong Address (Failure Diagnosis: Good = Defective)	3.1.2 Software Faults (Errors)	
1.2 Computer Software Failures (Faults)	2.1.3 Bus Controller Unit Failure - Site Selection Error	NOTE: Typical Failures Include:	
1.2.1 Failure to Isolate Faulty Entity	2.1.3.1 Multiple/Redundant Controller Selection - Hardware Arbitration	o Hardover to Max/Min Values o Steady Zero Values o Bias Offset o Reduced Dynamic Response o Sensitivity Change	
1.2.2 Isolation of Good Component as Failed	2.1.3.2 Multiple/Redundant Controller Selection - Software Algorithm Fault (Error)		
1.2.3 Processing Erroneous Data	2.1.3.3 Non-Centralized Controller Hardware Time-Out (Output Stage) Failure		
1.2.4 Failure to Complete Task - Exceed Task Time Allocation	2.1.4 Improper Decoding/Encoding of Address, Command, Data Word Structures		
1.2.6 Observability			

Table 9-1 DIGITAL DATA BUS SYSTEMS FAILURE MODES AND EFFECTS

The following considerations must be made concerning the possible failures of digital data buses: (1) transmission failures that may occur; (2) the effect on subsystems that are connected to the data bus by a bus controller or remote terminal failure; and (3) the effect of multiplex hardware failure. The navigation system must be self-contained and the aircraft must not become "lost" because of any type of transient. These safety requirements lead to subsystem requirements to store critical data in multiple locations and to recover rapidly from failures and upsets.

The three failure modes are: (1) no transmission; (2) incorrect transmission; and (3) failure to relinquish control. A fault with these failure modes and some of the related causes is shown in Figure 9-1. These failure modes are discussed in further detail in this paper.

Transmission Error

If the multiplex terminal hardware detects either an invalid word or a transmission discontinuity, the word and message are to be considered invalid. This message invalidation requirement may cause some systems (i.e., electrical multiplex (EMUX)) a problem. Since the EMUX systems usually have bit-oriented data rather than word or multiple words (message) oriented data, errors in a word following the reception of good data will invalidate good data. Message completion failures should always be detected in a multiplex system and are detected by the bus controller by either the suppression of the status word or the setting of the message error flag in the status word. The message error flag removes ambiguity as to whether the error occurred before the message was validated by the remote terminal or in the response to the message. Data transmission errors are handled by special error-handling interrupt software. The software will indicate whether (1) the command is to be retried, (2) the bus is to be used for the retry, and (3) whether the transmitted data (if any) should be invalidated. Tables 9-2 and 9-3 show the error identification types and the corresponding failure classes and error correction techniques.

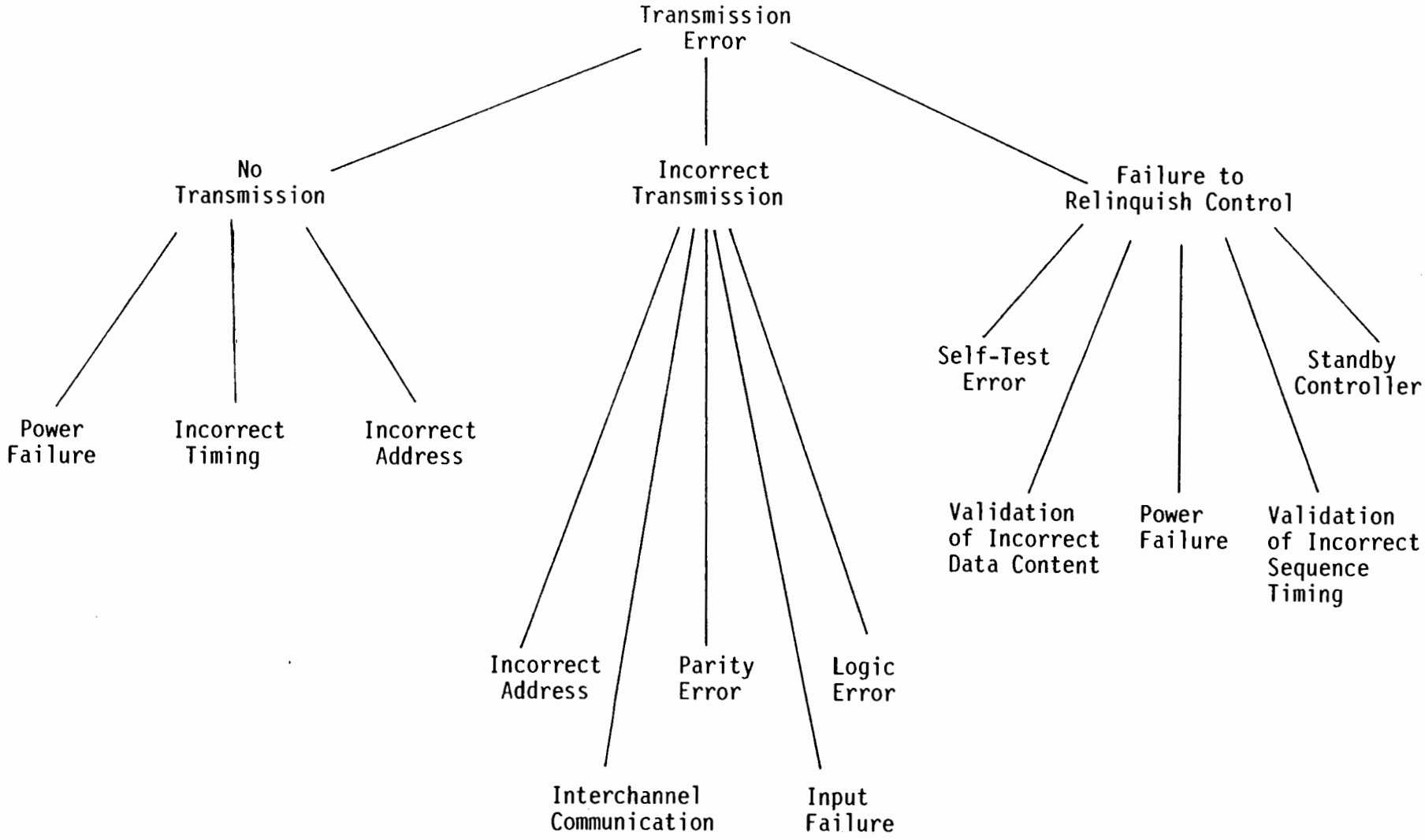


FIGURE 9-1 SIMPLE FAULT TREE EXAMPLE

ERROR IDENTIFICATION	BUS SYSTEM	SENSOR
a) Message error	Transmission from bus controller to to terminal was decoded with error condition by receiving remote terminal	--
b) Busy	Remote terminal unable to transmit or receive data at this time	Remote terminal and sensor unable to transmit or receive data at this time
c) Subsystem flag	--	Sensor failure preventing proper sensor actions
d) Terminal flag	Remote terminal failure preventing complete action by terminal	Remote terminal portion of sensor interface has failure preventing complete action by terminal
e) Parity error (incorrect odd parity)	Error in status word; data not usable	Error in status word; data not usable
f) Improper sync	Unknown problem -- ignore; continue to look for valid sync	Unknown problem -- ignore; continue to look for valid sync
g) Invalid manchester	Error in message -- ignore data in message	--
h) Improper number of data bits and parity	Error in message -- ignore data in message	--
i) Discontinuity of data words	Error in message -- ignore data in message	--
j) No status word response	Unknown problem -- requires further investigation	Unknown problem -- requires further investigation to achieve error

Table 9-2 FAILURE CLASSES [MIL-STD-1553B]

ERROR IDENTIFICATION TYPES	ERROR CORRECTION TECHNIQUE
1. Bus system failures a) No status word response b) Message error c) Parity error d) Invalid manchester e) Improper number of data bits and parity f) Discontinuity of data words	 Retry message on same bus n times Retry message on alternative bus n times Transmit status word mode code on each bus If necessary, transmit initiate self-test mode code Transmit BITE mode code Analyze failure and determine corrective action, which may involve the following mode commands: Shut down transmitter Inhibit terminal flag bit Transmit reset remote terminal mode code
g) Busy	Retry message on same bus after a fixed delay time
h) Terminal flag	If necessary, transmit initiate self-test mode code Transmit BITE mode code Analyze failure and determine corrective action, which may involve the following mode commands: Shut down transmitter Inhibit terminal flag bit Transmit reset remote terminal mode code
i) Improper sync	Ignore and reset for valid sync
j) Subsystem flag	Normal data communication messages (address/subaddress) to examine sensor BITE discretes or words
2. Sensor failure a) Discretes b) BITE data word(s)	 Analyze failure and determine system-oriented corrective action

Table 9-3 TYPICAL ERROR-CORRECTION TECHNIQUES [MIL-STD-1553B]

No Transmission

The user should listen to the bus it transmits on for its request address. If no bus controller activity is detected, the user should transfer listening to the other bus for its request address. If no activity is detected on the other bus, the user should continue toggling between the buses in search of bus controller activity.

Incorrect Transmission

The most serious failure for the bus controller is erroneous transmission. An independent frequency source should be used by the bus controller to provide monitoring and detection of transmission frequency faults. The two common types of transmissions are broadcast (which is sent on all of the channels) and command response (which is sent to a specific address). An error in a broadcast transmission has the potential for system failure if it is incorrectly validated at each of the addresses. An error in a command response has a more limited effect since it only involves one address. Each receiver should incorporate isolation provisions to ensure that the occurrence of any reasonably probable internal line replaceable unit (LRU) or bus receiver failure does not cause any input bus to operate outside of its specification limits (both undervoltage or overvoltage).

Failure to Relinquish Control

Subsystem or terminal failures may be detected using built-in test (BIT) circuitry. These failures are reported by the setting of the subsystem flag bit or the terminal flag bit in the status word. In aircraft, dual-redundant buses are used, so a terminal failure may be isolated to one bus. Depending on the capability of the remote terminal hardware, the transmit BIT word mode code can be a powerful diagnostic aid. For each fault, the action to be taken must be determined, designed for, and implemented by the system.

Subsystem or terminal failures can also be detected without the use of the optional terminal or subsystem flags. Bad data or non-varying data from a subsystem may be interpreted as a subsystem failure. Repeated message completion failures to a remote terminal via all possible data paths could be considered as a loss of the terminal functions. The system software should be used to detect these failures.

Bus controller operation in the event of failure is important to an integrated data bus system. The primary bus controller should relinquish bus

control whenever it suffers a power interruption of a power supply which might cause erroneous outputs. The primary bus controller should detect its own bus control processing faults and remove itself as controller in a fail-passive manner. Similarly, the backup bus controller should recognize invalid control messages or the absence of valid control messages and revert to active bus controller status. Monitoring techniques should provide coverage for both hardware faults and software errors. Any undetected fault in the primary bus controller which results in continuous erroneous transmission will make all standby controllers ineffective. The bus controller is structured such that two independent faults must occur in order to cause erroneous transmissions.

Reliability for Flight Safety

Flight safety requirements allow no more than one unrecoverable failure in the flight control subsystem per 10^9 flights. This failure rate is consistent with AC-25-13091 and is appropriate for integrated systems. The failure rate must encompass the entire flight control system including the necessary supportive electrical power, hydraulics, and any other subsystem used in the flight-critical capacity. When applied over the two and three hour mission duration of the aircraft, a maximum failure rate of approximately 5×10^{-6} failures per flight hour (for a two hour mission and 3.3×10^{-6} failures per flight hour (for a three hour mission) can be allowed.

Figure 9-2 gives an example for the determination of the loss of bus control. The potential failures for the bus control example are given in Table 9-4. The total failure rate must be equal to or less than the total allowable defined above. In the example, the loss of bus control, D_1, is

$$D_1 = (E_1 + E_2 + E_3)(E_4 + E_5 + E_6) + E_7 + E_8 + E_9 + E_{10}$$

By substituting in the values from Table 9-4, we obtain $D = 3.1012321 \times 10^{-5}$. Therefore, in this example the data bus would fail to meet the reliability requirements for flight safety.

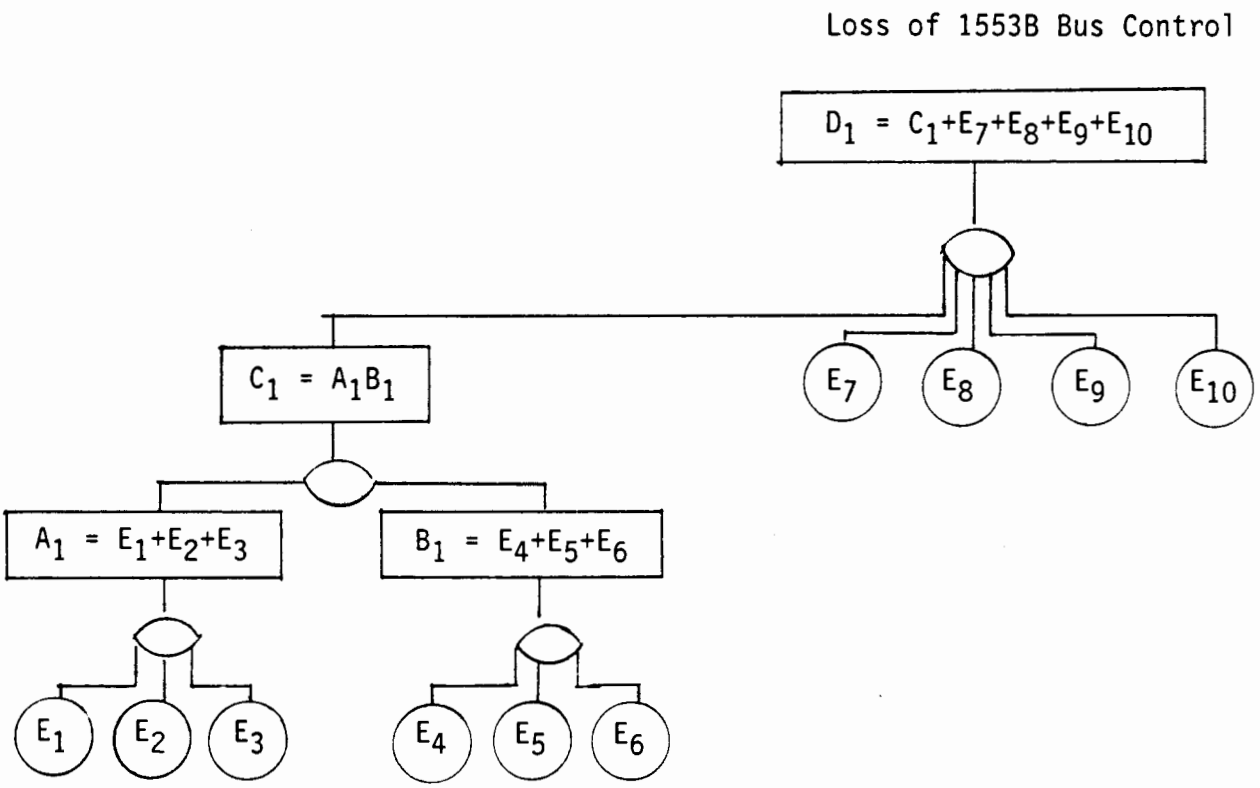


FIGURE 9-2 SINGLE CHANNEL-DUAL OUTPUT (BUSES A AND B) BUS CONTROL

ERROR	ERROR SOURCE	FAILURE RATE (λ)
E_1	Bus A - Transformer Failure	10^{-6}
E_2	Bus A - Transceiver Failure	10^{-4}
E_3	Bus A - Decoder Failure	10^{-5}
E_4	Bus B - Transformer Failure	10^{-6}
E_5	Bus B - Transceiver Failure	10^{-4}
E_6	Bus B - Decoder Failure	10^{-5}
E_7	Single Encoder Failure	10^{-5}
E_8	Internal Control Logic Failure	10^{-5}
E_9	Interface Unit Failure	10^{-5}
E_{10}	Microprocessor System Failure	10^{-6}

Table 9-4 POTENTIAL FAILURES RESULTING IN LOSS OF BUS CONTROL SINGLE CHANNEL - DUAL OUTPUT (BUSES A AND B)

10.0 FIBER OPTIC DATA BUS FOR AVIONICS INTEGRATION

As stated in previous sections, the bus topology is the physical arrangement and interconnection of the various terminals. In a fiber optic bus, the elements utilized are: optical couplers; fiber cable; connectors; and splices. The design of these elements not only relates to system performance but also to system installation and maintenance. Because optical power losses occur whenever any of these components or functions are inserted in the optical path, performance is affected. Table 10-1 presents the components and factors which influence the limits of optical bus technology as it applies to optical buses used for avionics integration.

Optical Path

Basically, the optical path is the fiber optic cable. In designing the proposed avionics architecture, the fiber cable must be selected for minimal loss (across the bus) and wide bandwidth. In addition, the fiber cable must be constructed for strength and endurance during the life of the bus architecture; ease of installation; and long term environmental performance.

Splices and Connectors

Interconnections between the fiber cable elements (controllers, remote terminals, junctions, etc.) can be made with either splices or connectors. Splices in the fiber cable are easier to incorporate and provide lower losses than connectors; however, splices are permanent. Connectors, on the other hand can be mated/unmated hundreds of times with virtually no degradation in performance. Therefore, in the development (and design) of a fiber optic based avionics architecture optical couplers (connectors) should be utilized for bus interface connections to the physical bus to minimize downtime due to repair and/or changes to the architecture structure or implementation induced by adding or deleting remote terminals or at the avionics boxes to the physical bus.

In the case of aircraft having pressurized bulkheads, several penetrations through these bulkheads may need to be made. At these penetrations, the fiber optic cable can either be run "straight-through" the bulkhead or an optical connector (coupler) can be used on each side of the bulkhead. The tradeoff, in this case, is between the ease of installation

and rework using a connector (coupler) system or the lower loss and absence of reflections using a spliced or through cable.

Table 10-2 deals with the concerns and issues associated with the implementation of a high integrity fiber optic cable based avionics architecture.

COMPONENT	FACTORS
o Couplers	Losses Number of Taps
o Fiber	Fiber Type Modal Noise Connectors Splicing Reflections Cabling
o Optical Source	Power Speed
o Optical Receiver	Sensitivity Intermessage Dynamic Range Intermessage Response Time Clock Recovery
o Processing/Interface Logic	Speed Power Consumption VHSIC/VLSI & GaAs
o Topologies	Performance Reliability Flexibility Installation and Maintenance
o All	Cost

Table 10-1 OPTICAL BUS TECHNOLOGY LIMITS

OPTICAL COUPLERS

The two basic types of optical coupling techniques which are considered for an optical data bus are star couplers and taps or tees.

A. In a transmissive star, N ports are designated as input ports, and N ports as output ports. The optical energy on any input port is split more or less equally between all output ports, with a splitting loss of 10 log N. Star couplers also have an insertion loss and a port-port variation of 1-3 dB each depending on the number of ports. Stars in excess of 100 ports have been fabricated; however, for minimal cost and port-port variations, the practical limits of current technology is 64 ports.

B. Directional couplers for tapping a transmitter and receiver onto a fiber optic bus are basically like a 4 port star transmissive star with an excess loss of 0.5-1 dB. Typically a tap into the receiver can be accomplished with a 90/10 or 95/5 split providing 0.5-2.0 dB link throughput loss, respectively, and a 10 dB to 13 dB tap-off or reduction of the link power into the bus receiver. For tapping the transmitter into the bus, the throughput loss as well as the coupled transmitter power reduction is 3 dB in commercially available couplers.

OPTICAL CABLES

Considerations involved in evaluating optical cables for a fiber optic data bus include fiber design (including modal noise and reflection effects) and cable type and construction.

Size

Of the available fiber options, the 100/140 micron or the 85/125 micron graded index fiber operating at 0.05 μm is optimum because:

(a) Their large core, high NA, and operation wavelength will support many more modes, thus minimizing the modal noise limitation.

(b) Their large core enables greater LED coupled power, thus extending the application of LEDs.

(c) Their core-clad geometry makes it easier to make low excess loss star couplers.

Table 10-2 CONCERNS AND ISSUES
(table continues)

Reflections

Another consideration in the media analysis is reflections. Reflections result from an index of refraction discontinuity at connectors, poor splices, or mismatched fiber types. For example, with a star coupler, the main signal passes through the link; however, part of the signal is first reflected at the star coupler dry connector (8%) and then again at the transmitter dry connector (8%). The resulting reflected signal is down 22 dB with respect to the main signal and delayed by 1 microsecond (1 nsec/meter). This reflected signal becomes a problem if it overlaps the next bus transmission and shows up as noise superimposed on this data. Therefore, consideration must be given to minimize reflections.

Connectors

Optical connectors which are suitable for use in a data bus are low cost, easily installed, and typically low loss. The connector loss depends on the fiber size as well as the quality of the connector. For 100/140 m fiber, losses vary from 0.5 to 1.5 dB depending on connector quality. Available multi-way connectors have the advantage of simplifying a bulkhead penetration and provide quicker connect/disconnect of a multi-fiber cable. Although there is no fundamental reason for higher loss in a multi-way connector, the losses in currently available connectors average approximately 0.5-1 dB more than the loss in a single fiber connector.

Splicing

For field installation, maintenance, and repair the elastomeric splicing system has been identified as the best currently available splicing technique.

TECHNOLOGY - OPTICAL BUS TRANSMITTERS AND RECEIVERS

Fiber optic bus T/R design is driver by the goal of maximizing bus efficiency. This is necessary to fully utilize the benefits of the bus, minimizing "dead" time, and allowing transfer of significant quantities of data.

An efficient bus transmitter and receiver are relatively easy to design. However, providing very quick transmitter power output stabilization and very short receiver settling time at the start of a message significantly increases the difficulty and complexity of the transmitter and receiver design. A fast response clock recovery scheme is also critical to minimizing

Table 10-2 CONCERNS AND ISSUES
(table continues)

the amount of time used for non-date. In summary, the more time used to perform overhead functions, the less time there is to transmit data, and the less the efficiency of the bus.

Maximizing Bus Efficiency

One of the principal considerations in maximizing bus efficiency revolves around the unique aspects of an optical transmission. Intensity modulation of an optical carrier provides a unipolar transmission channel, unlike electrical current transmission over wire which may be bipolar. Unipolar signaling causes a DC shift between signal-on, and signal-off states, which will disturb the operation of conventional receiver amplifiers having AC coupling until the interstage coupling capacitances have had time to accommodate the shift. A similar DC shift occurs between small and large signals.

Thus to avoid a long settling time at the start of messages, receivers designed for data bus application either have a short AC coupling time constant to minimize the disturbance time, or DC coupling is employed, in which case more complex circuitry is required for setting the data decision threshold for the received waveform. The shift in average power between signal and no-signal states also complicates laser optical source power stabilization, which is normally accomplished using average power feedback control.

Transmission Losses

Optical bus configurations have considerable, and somewhat undefined transmission losses between source and detector, resulting from the coupler(s) and connectors. When combined with source power and detector sensitivity variations, this gives rise to an uncertain received power level. A high gain wide dynamic range receiver is required and again since time is a premium, long term averaging of undesirable. Alternative methods for rapidly accommodating the dynamic range are required, and this is a major concern of optical data bus receiver design.

Receiver Losses

Three receiver types are known which provide simple, instantaneous adjustment to message levels. In the symmetrical clamp receiver all signals are bit-by-bit clamped to the same low level and after amplification, data decisions are made with a fixed threshold. Good dynamic range can be achieved and no start-of-message time constant delays are experienced, unlike conventional linear or limiting receivers. The technique operates well up to

Table 10-2 CONCERNS AND ISSUES
(table continues)

bit rates around 50 Mb/s, above which implementation problems arise (the upper bit rate limit may be extended using lower capacitance hybrid construction). This technique is a leading candidate for receivers operating at lower data rates.

A second fast response scheme uses a DC coupled receiver (to avoid AC coupling time constants) and a bit-by-bit adaptive threshold decision. The technique is ideally suited to very high data rate reception but dynamic range is limited by amplified design. Optimum performance is limited by DC offset in the amplifier, which may be a limitation for wide temperature range operation.

High bit rate reception may also be handled efficiently with a high pass filtering receiver when the signal is any biphase code, or other reduced low frequency content code because required coupling capacity time constants become small compared to the fixed bus inter-message dead time resulting from propagation delays. Appropriate filters have been designed with a linear phase response in the stop band, providing an intermessage response time as low as 6 bit times for Manchester coded data.

Conventional point-to-point system optical receivers have well defined sensitivity limits which may be calculated from thermal and shot noise of the devices. For data bus receivers, a number of compromises in design are necessary to achieve fast response to messages, and these generally result in less sensitivity. Similarly, wider dynamic range may generally be achieved in a receiver which has a long period to adjust to changes in signal level than in a data bus receiver which is required to adjust almost instantaneously.

The receiver sensitivity is affected largely by the type of photodetector and preamplifier design. A silicon avalanche photodetector offers greatest sensitivity (at 0.85 micron) and preamplifier design is less critical. At 0.85 micron, a silicon PIN diode with a sensitive preamplifier has approximately 10 dB less sensitivity.

Transmitter Losses

For relatively low rate transmission, i.e., <10-50 Mb/s, little difficulty exists in designing a transmitter circuit using LEDs. Data modulation may be DC coupled through to the LED and any data format or message length may be accommodated. Very high data rate transmission requires the use of a semiconductor laser diode to achieve the required modulation rate and sufficient launched optical power to provide reliable

Table 10-2 CONCERNS AND ISSUES
(table continues)

reception after the transmission losses. Lasers require a more complex driver circuit to ensure that the drive current is compensated for temperature and aging of the source, and is correctly prebiased during transmission to avoid data distortion resulting from lasing turn-on delay. Effective compensation of the drive current requires feedback control of the launched signal, which commonly operates by stabilizing the average transmitted power in continuous transmission point-to-point systems. With the burst nature of transmission in a bus system, averaging is not as convenient, and requires a long preamble for the laser power to initially stabilize.

Any data bus transmitter design must include an override control, which provides a positive curtailment of transmission in the event of a latch-on fault. An external timeout circuit or protocol function controls this override function.

OPTICAL TRANSMITTER/RECEIVER POWER MARGIN

A key element in the design and optimization of any fiber optic link including a data bus is the system power budget analysis. Such an analysis is important not only to ensure that there is adequate optical power at any giver receiver under all conditions, but to also ensure, particularly in a data bus, that there is not too much optical power at any given receiver.

There are three basic elements to a power budget analysis: system losses, optical source output power, and optical receiver sensitivity. The latter two elements were discussed above. The system losses for various topologies will be presented in the following section. The maximum allowable system loss can be derived for a transmitter combined with a realizable receiver. Output powers of -6 dBm can be achieved with high radiance LEDs coupled to 100 m core fiber with an NA of 0.3.

TOPOLOGY ANALYSIS

Using the practical technology/implementation limits as discussed in the previous sections, an analysis of various fiber optic data bus topologies or configurations was performed to evaluate the number of terminals possible at various data rates.

Table 10-2 CONCERNS AND ISSUES
(table continues)

The topologies examined included:

(a) Linear
  Inbound-outbound (loop or ring)
  Bidirectional (open-ended)
  Active

(b) Star
  Transmissive
  Reflective
  Star-star
  Active star-star

(c) Hybrids
  Star-loop
  Loop-star

Since active stars and active rings are essentially point-point links, bus losses are not the limiting factor on the number of terminals, nor is dynamic range a factor in receiver design.

For this initial, first order analysis, the best case performance for splices, connectors, and couplers was assumed. This approach "brackets" the problem by defining the best possible performance of a particular topology implemented with currently available/near term technology.

A passive transmissive star bus is the most efficient topology because the power from any transmitter is distributed evenly between all receivers. In addition, there is only one coupler insertion loss in between any given transmitter and receiver.

The principal disadvantage of a bus with a single star is that the cables from all T/R modules must be run to the star. In an aircraft, this increases the initial installation cost due to the increased number of bulkhead penetrations required. In addition, there is little flexibility for adding new terminals at arbitrary locations. One solution to this is to provide a distributed bus topology such as a star-star or a star-linear topology. The performance of the star-star topology can be easily improved by adding a single repeater (or two for redundancy) at the central star.

Two hybrid topologies combining stars with a linear bus concept were investigated because they provided four separate nodes with the potential of improved performance over a simple linear bus. The first is a star-loop, the second a loop-star.

Table 10-2 CONCERNS AND ISSUES
(table continues)

Initial analysis of these revealed very little reduction in bus loss over a simple linear loop and therefore a detailed analysis was not performed. The loop-star or distributed star topology can be effective, however, with active repeaters between the stars.

The only viable passive topology for 128 terminals is a star; however, an active linear bus, active star, or active star-star are viable implementations for 128 terminals at 300 Mb/s. The latter, the active star-star, appears optimal because it:

(a) Minimizes cabling/bulkhead penetrations with 4 (or more) nodes for concentrated locations of terminals which also enhances flexibility.

(b) Minimizes number of repeaters and therefore cost/maintenance.

(c) No single point failure will disable the entire bus.

(d) Allows use of star couplers with 6-32 ports, thus reducing the cost and increasing the performance/reliability of the couplers.

Table 10-2 CONCERNS AND ISSUES

Fiber Optic Network Based Losses

A typical set of requirements for an avionics multiplexed bus of a commercial transport could include anywhere from 32 to 128 terminals, and data rates could be in the 10-100 MHz (or million bits per seconds) range. The bus probably would be bi-directional, using a broadcast type mode in which any terminal might transmit data to any other terminal in the network. Various topologies for such a bus have been discussed earlier; however, the most probably topology for such an architecture would be a star-coupled topology due to the fact that it can be implemented without the use of active repeaters which would result in higher reliability, lower maintenance, and reduced losses in the optical path.

Table 10-3 presents a typical loss budget calculated for an approximately 60 terminal star-coupled transmission network. From this table, it can be seen that the bus network will require high optical output from the transmitter and high receiver sensitivity to assure that the integrity of the data is maximized. In order to insure the high integrity, the bus optical components will have to be selected to be consistent with simple straightforward system design at both the transmitter and receiver ends.

COMPONENT	MINIMUM LOSS	MINIMUM LOSS	COMMENT
Fiber	0.0 dB	1.0 dB	50 m. terminal to star maximum, 5 dB/km
Connectors	0.4 dB	8.0 dB	.1 dB to 1.0 dB each, 4 to 8 total terminal to terminal
Star Coupler	17.1 dB	21.1 dB	Typical
TOTAL	17.5 dB	30.1 dB	
Optical Dynamic Range: 12.6 dB			

Table 10-3 STAR-COUPLED NETWORK LOSSES

11.0 IMPACT ON CERTIFICATION CRITERIA

Rapid advanced in microelectronics, digital data bus technologies, and software will provide more fault-tolerant digital data bus architectures which operate at higher speeds with greater bandwidth. These advances will impact the information needs of the FAA for the purpose of certifying the safety of systems utilizing these technologies. This section discusses issues which should be considered in modifying certification criteria and regulations relevant to the safe operation of aircraft.

Transmitted Data Necessary to Assure System Safety

Safety requirements as specified in AC 25.1309-1 dictate the reliability and fault tolerance of a system design providing or involved in flight critical functions (functions which would prevent the continued safe flight and landing of the aircraft if not properly accomplished). This means that any data transmitted over a digital data bus must meet these requirements. All components, both hardware and software, required for provision of a flight critical function must be considered in any analysis. Any failure which results in a loss of a flight critical function must be shown to be extremely improbably (less than 10^{-9} probability of the event occurring per flight hour). In order to achieve this low value, the flight critical functions must, as a minimum, be shown to fail operationally. A single point failure cannot be permitted to occur if it cannot be shown that such a failure will have no impact on safety. This means that faults which can impact safety must be detected and recovered from within the control system sampling time subject to the constraints imposed by the system time constant. A rule of thumb for selecting sample rates is that a rate of at least five times per time constant is a good choice.

Architectural Variations Impact on Safety/Reliability

The reliability and safety are a directional function of the architecture of the data bus network. As previously shown, different levels of redundancy are required using the same bus system components in order to achieve required levels of reliability. Of course, a point of diminishing return can be reached until the overall system reliability actually decreases as additional redundant components are added. Another factor which must be kept in mind in selecting an architecture is the amount of time to detect and

recover from a fault. Recall that the time to switch out a faulty node in a token passing ring is significantly greater than that needed for a linear token passing bus.

Assurance Assessment Methodologies to be Conducted/Completed to Assure System Safety

At a minimum, the equipment involved in flight critical functions should be subjected to the environmental test procedures and test conditions contained in Radio Technical Commission for Aeronautics Document DO-160A, as noted in AC21-16. Equipment failing these tests should not be approved. Note that these tests are only designed to determine the performance and not the service life or mean-time-between-failure (MTBF) or failure rate.

Equipment manufacturers should be required to provide proof of failure rate data for each component, including the method utilized to estimate the failure rate. A fault tree should be derived for each function whose performance impacts flight safety. The failure rates used in these fault trees should be the same as that provided by the manufacturer. A mission scenario should be used to derive the mission timeline for all flight critical functions and hence the determination of the exposure time to be used in the fault tree calculations.

A similar process should be followed for the software involved in the flight critical functions. The problem that surfaces here is that no widely accepted method exists to estimate the failure rate of a software module, since there are many factors that impact faults due to software, including the incorrect or incomplete statement of the software requirements which could result in a required function not even being designed or implemented.

The use of real-time simulation with actual hardware and software in the loop should be required with automatic injection of probable faults (permanent or transient) by a test control program using as inputs test vectors automatically generated by validated and approved support software.

This should be followed by the mandatory flight test of the system to demonstrate its ability to detect and recover from faults which may only occur in the airborne environment and cannot be duplicated on the ground or in the laboratory.

Fault Insertion Levels for Detection and Recovery from Immediate and Latent Faults in Bus Architectures

As previously described, there are many faults in a bus architecture which must be detected in order to achieve the level of fault tolerance required for systems performing flight critical functions. No matter what the architecture, the need exists to verify that the bus cannot be jammed by a malfunctioning node, nor can required transmission cease to occur due to a malfunction of a hardware or software component. This dictates being able to insert a simulator for a node which can either function as a bus controller for buses having a centralized control, or as a remote terminal which inserts faults data, fails to relinquish control, or fails to transmit in its time slot.

The simulator should be capable of simulating both hard and transient faults under control of software independent of the information being transmitted over the data bus. Stuck at faults, shorted, and open devices should be capable of being simulated.

In addition, the performance of actual devices used on the bus should be determined while they are subjected to environmental disturbances, such as input power fluctuations.

Acceptable Data Package for Certification of a Specific Architecture

The data package for certification of a specific architecture must contain, at a minimum, the following:

a) System/Segment Specification
b) Software Requirements Specification
c) Interface Requirements Specification
d) Software Standards and Procedures Manual
e) Software Development Plan
f) Software Configuration Management Plan
g) Software Quality Evaluation Plan
h) Software Top Level Design Document
i) Software Detailed Design Document
j) Interface Design Document
k) Software Test Plan
l) Software Test Description
m) Software Test Procedure

n) Software Test Report

o) Environmental Test Plan

p) Environmental Test Result Report

Some of these data items could be combined, resulting in fewer numbers. Regardless of the form, all of the information should be provided for the purpose of certification.

High Speed (10 MHz - 100 MHz) Data Bus Impact on Certification Criteria

The introduction of high speed data buses will not impact certification criteria. No matter what the speed, or architecture, the manufacturer must satisfactorily prove that the bus will not impact the safety of the aircraft flight critical functions.

Coaxial and Triaxial Cable Transmission Media Impact on Existing Certification Criteria

The type of transmission media impacts the instrumentation needed to measure signals being transmitted over the media. Electromagnetic compatibility (EMC) must be demonstrated through the tests prescribed in DO-160A. Tests in DO-160A include magnetic effect, power input, voltage spike conducted, audio frequency conducted susceptibility, induced signal susceptibility, radio frequency susceptibility (radiated and conducted), and emission of radio frequency energy. Computer-aided EMC analysis can also be useful to analyze intrasystem EMC prior to the system being fully integrated. Changing the transmission media from twisted pair to coax or triax does not impact existing certification criteria. The introduction of fiber optic cable should not change the criteria but will create the need for development of tests designed to determine the performance and reliability of the fiber optic cable in these applications.

Certification Issues

The primary impact of new technology will be the need to rely more on formal specifications and simulation than has been necessary in the past. Due to the inability to inject every possible fault and demonstrate recovery from all single faults, let alone concurrent faults, simulation will be needed to verify the systems fault tolerance. The development of expert systems will pose an interesting certification issue, particularly if they are providing advice to the pilot, which is based upon inferences drawn from knowledge bases using rules developed by non-experts. Even if experts are

used, the challenge of certifying an expert system should not be underestimated.

BIBLIOGRAPHY

1. Chow, K.K., W.B. Leonard, and T.C. Yang. A wavelength division multiplex (WDM) optical data base for future military applications. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

2. Stanislaw, David L. (Cessna Aircraft Co.). General aviation gets a data bus update. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

3. Penn, D., S. Levy, and E. Loker. A standard computer bus for MIL-STD-1750A avionics computers. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

4. Spieth, J.E. (WPAFB, Ohio). Data bus interface MIL-STD-1553B/ARINC 561. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

5. Yount, L.J. (Sperry Corp.). Architectural solutions to safety problems of digital flight-critical systems for commercial transports. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

6. Lala, J.H. (Charles Stark Draper Labs). Advanced information processing system. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

7. McNamara, Brian J. (ARINC Research Corp.). AI concepts in MUX bus control: Layered reservation access. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

8. Mehl, Byron, and Gary Pierle (Sunstrand Aviation). A minimum interruption AC electrical power generating system for avionics. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

9. An overview of the digital avionics assessment activities being conducted by the Federal Aviation Administration at NASA-Ames Research Center. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

10. Doleler, Quentin (Johns Hopkins University). High speed bus structures for multiprocessing. Proceedings of the 6th AIAA/IEEE Digital Avionics Systems Conference, 1984.

11. Thomas, Ronald E. (Sperry Flight Systems). A standardized digital bus for business aviation. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

12. Lancaster, Phil (Smiths Ind.), and Brian Middleton (D&O Engineering). Multiplexing utilities in general aviation aircraft. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

13. Card, M. Ace (Bendix). Evolution of the digital avionics bus. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

14. Martin, George (Beech Aircraft). Making the digital cockpit operational in general aviation aircraft. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

15. Bondy, John, and Richard Weaver (G.E. Space Div.). Bus schedule change issues in the On-Board Distributed Data System (ODDS). Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

16. Bennett, Donald (Sperry Corp.) The V Bus Family: Candidate for common use with VLSI technology. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

17. Husbands, C.R. (Mitre Corp.), and R. Katz (Naval Avionics). The application of multiple speed data rate transmission on a MIL-STD-1773 data bus structure. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

18. Leonard, William, and Kungta Chow (Lockheed Palo Alto). A new bus architecture for distributed avionic systems. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

19. Wilent, C.E. (TRW Military Electronics Division). Directions in avionic data distribution systems. Proceedings of the 5th AIAA/IEEE Digital Avionics Systems Conference, 1983.

20. Ferrell, P.J., and M.D. McFarland (Boeing Military Airplane). Computer-in-control selection logic for a triplex digital flight control system. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

21. Chun, Randall (Boeing Aerospace). ARINC 429 digital data communications on the Boeing 757 and 767 commercial airliners. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

22. Lindsay, T.A. (Boeing Aerospace). A fiber optic interconnection of two MIL-STD-1553B data buses. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

23. Wilson, D.H. (Vought Corp.). A polled contention multiplex system using MIL-STD-1553 protocol. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

24. McCuen, James (Hughes Aircraft). Higher order information transfer systems are coming. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

25. Kincaid, B.E. (Lockheed Palo Alto). Advanced fiber optic systems for avionics applications. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

26. Lavin, H.P., and G.B. Harrold (General Electric). Light-guided information distribution systems. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

27. Brock, L.D., A.L. Hopkins, and J.L. Spencer. On-board communication for active-control transport aircraft. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

28. Zaman, M.K. (Lockheed-California). Fiber-optic immunity to EMI/EMP for military aircraft. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

29. Brumback, B.D. (General Electric). Time-referencing of data in an asynchronous environment. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

30. Thullen, M.J. (WPAFB, Ohio). Advanced weapon systems-integration technology. Proceedings of the 4th AIAA/IEEE Digital Avionics Systems Conference, 1981.

31. Moning, Russ, and G. Hill (Boeing Military Airplane Co.). Fiber optic high speed data bus. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

32. Folmar, R.J. (Harris Gov. Aerospace System Div.). Distributed memory network: An 8 gigabit fiber optic tightly coupled system. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

33. Uhlhorn (Harris Corp). Imaging connector interconnect system for a parallel fiber optic data bus. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

34. Varga, Michael P. (Sperry Aerospace). A robust 100 MBPS network for avionics applications. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

35. Couch, P.R., and K.D. Ferris (Fibercom, Inc.). High speed fiber optic data bus for avionics integration. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

36. Ludvigson, M.T., and K.L. Milton (Rockwell Intl. Corp.). High speed bus for pave piller applications. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

37. Alber, H.J., and W.A. Thomas (WPAFB, Ohio). A dual channel high speed fiber optics multiplex data bus system. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

38. Freidman, Steven N. (ILC Data Device Corp.). MIL-STD-1553 programmable dual redundant remote terminal, bus controller, bus monitor, unit. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

39. Nagaki, Junior A. (Boeing Aerospace Co.). Development of a multilevel secure local area network. NAECON Proceedings, Vol. 1 (2), Vol. 2 (2), 1985.

40. Subramanyam, V.R., L.R. Stine, and V.W. Nicklow (TRW Military Electronics). High speed bus for CNI/EW applications. NAECON Proceedings, Vol. 2 (2), 1984.

41. Buckwalter, Len. General aviation gets a data bus. Avionics, April 1985.

42. Wood, T.G. (Lockheed-Georgia Co.) The high technology test bed (HTTB) program system description for the Digital Flight Control System (DFCS).

43. Mason, R.C., and L.D. Parriott (TRW). Standardization in military avionics systems architecture. Proceedings of the IEEE/AES-S Conference, 1979.

44. Cromer, Oscar M. (Westinghouse). The challenge for avionics systems design of the 80's - Control of the digital processing architecture explosion.

45. Moran, John F. (General Electric Co.). Integrated displays and controls for military aircraft. Proceedings of the 3rd Digital Avionics Systems Conferences, 1979.

46. Methods for verification and validation of digital flight control systems. December 10, 1984.

47. Candidate system development - Digital Autonomous Terminal Access Communication (DATAC), The Boeing Company (Proprietary), 1979.

48. DATAC draft. The Boeing Company, November 1, 1982.

49. Bannister, J.A., K. Trivedi, and V. Adlakha (NASA-Langley). Problems related to the interration of fault-tolerant aircraft electronic systems. NASA Report 165926, June 1982.

50. Avionics Standard Communication Bus (ASCB), The Sperry Corp.

51. Multibus avionic architecture design study (MAADS). TRW Defense/Space Systems for WPAFB, October 1983.

52. Mark 33 Digital Information Transfer System (DITS). ARINC Document - Aeronautical Radio, Inc., April 1981.

53. Ciasulli, Louis (Aydin Vector). A tutorial on MUX bus monitoring. October 1984.

54. Erwood, R.G., R.D. McCorkle, et al. (Boeing Aerospace). Digital flight control redundancy management system development program. May 1979.