Advanced Embedded Processing
Present and Future

The Boeing Company
G.C. Cohen

Integrated Airframe/Propulsion Control System Architecture (IAPSA II)

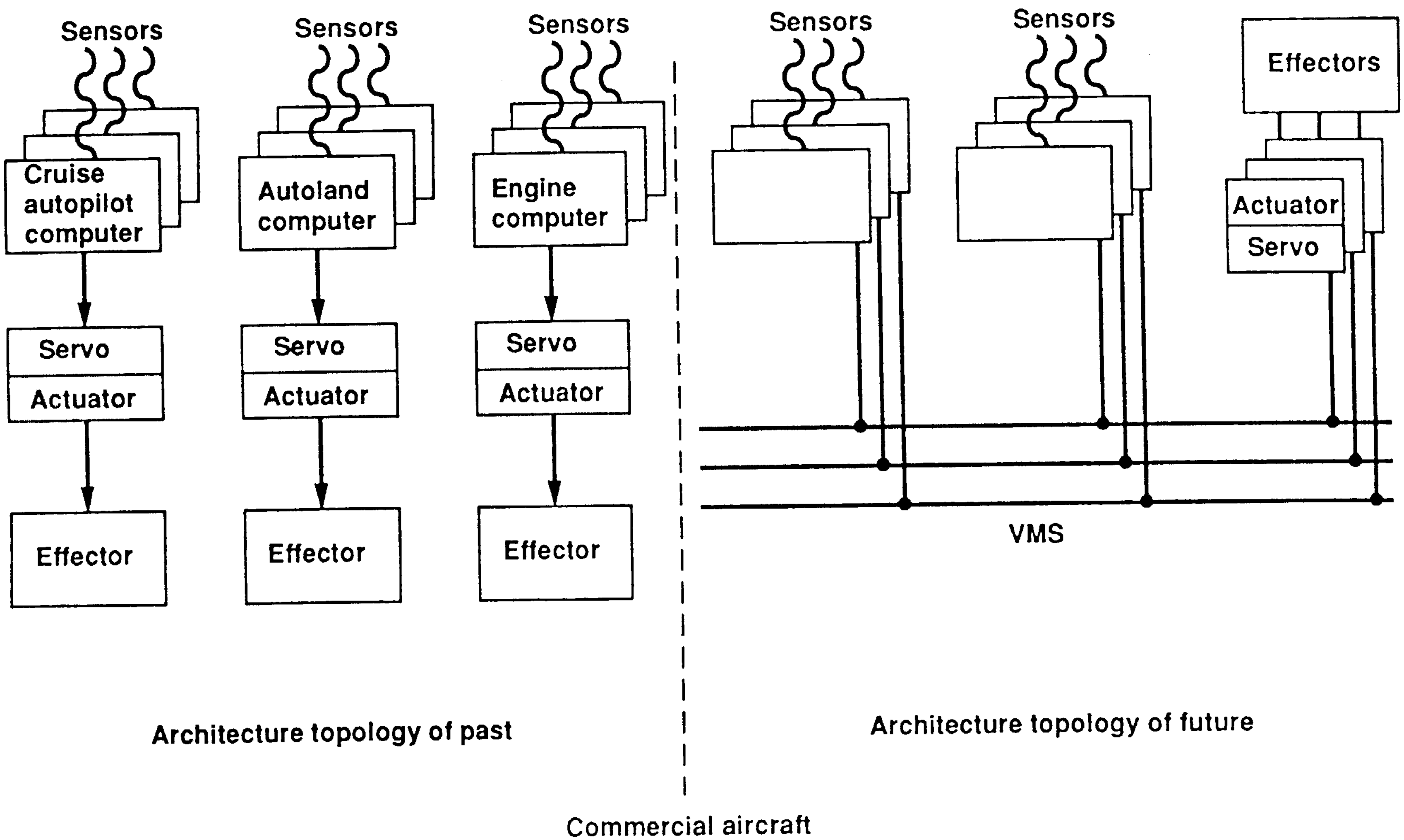
Began: July 26, 1985
Ended: April 1, 1990

Integrated Airframe/Propulsion Control System Architecture (IAPSA II)

Began: July 26, 1985
Ended: April 1, 1990

Methodology

Why a Methodology



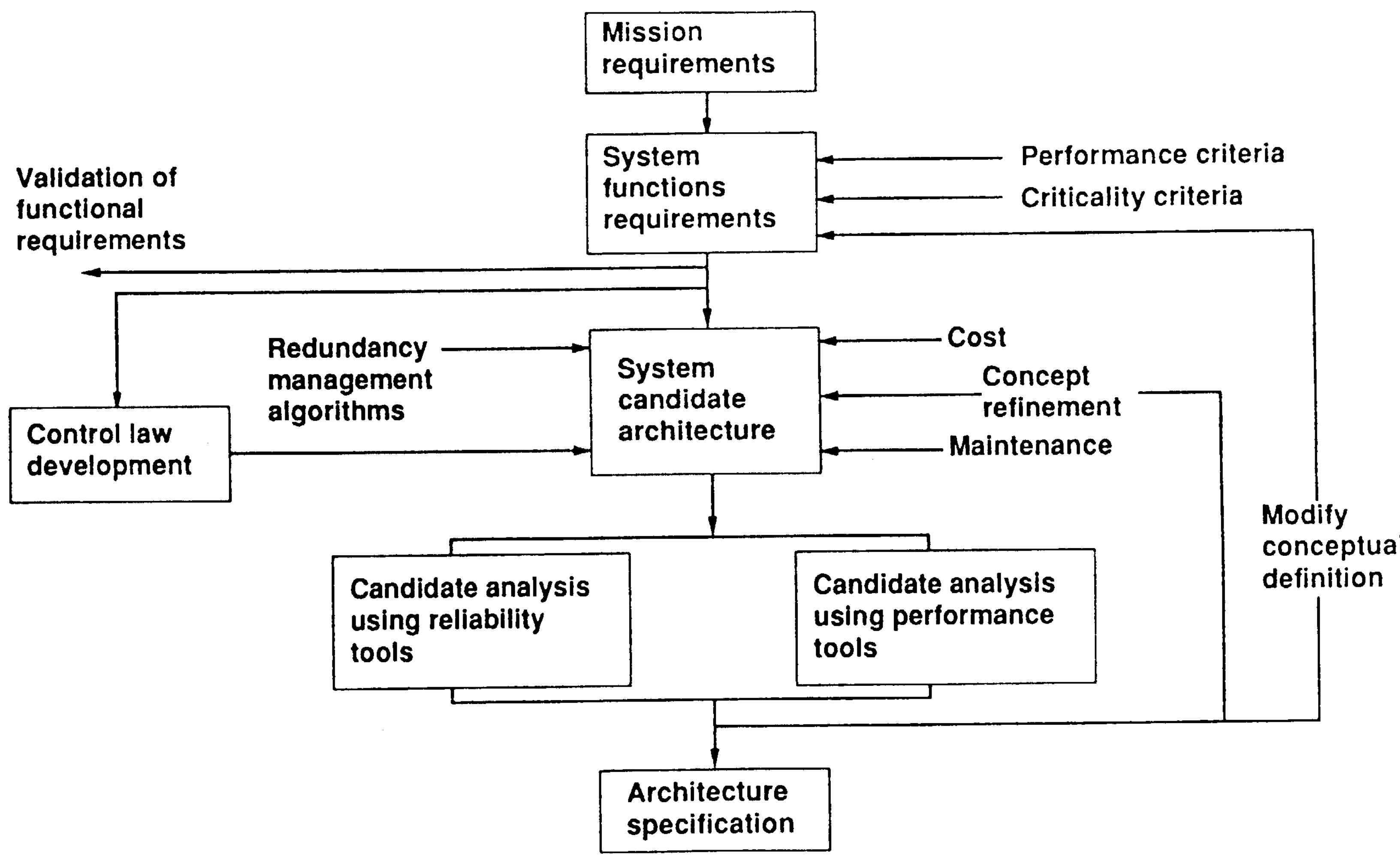
Problem

- Interrelationships difficult to specify in terms of meaningful requirements
  - Normal mode
  - Failure mode
- Unless contractor/vendor team takes a systems approach, system will be overdesigned and still may not meet the requirements

Methodology Elements

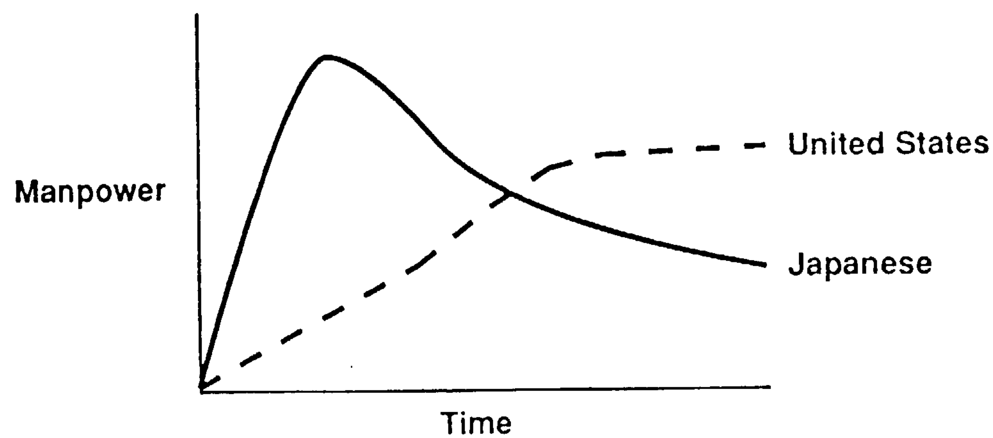
- Requirements
- Specifications
- Design
  - Automation
  - Guidelines
  - Building blocks
  - Reliability
  - Performance
  - Design for validation
  - Design for cost
  - Proof of correctness
  - Availability
  - Survivability
  - Maintainability
- Testing
- Traceability

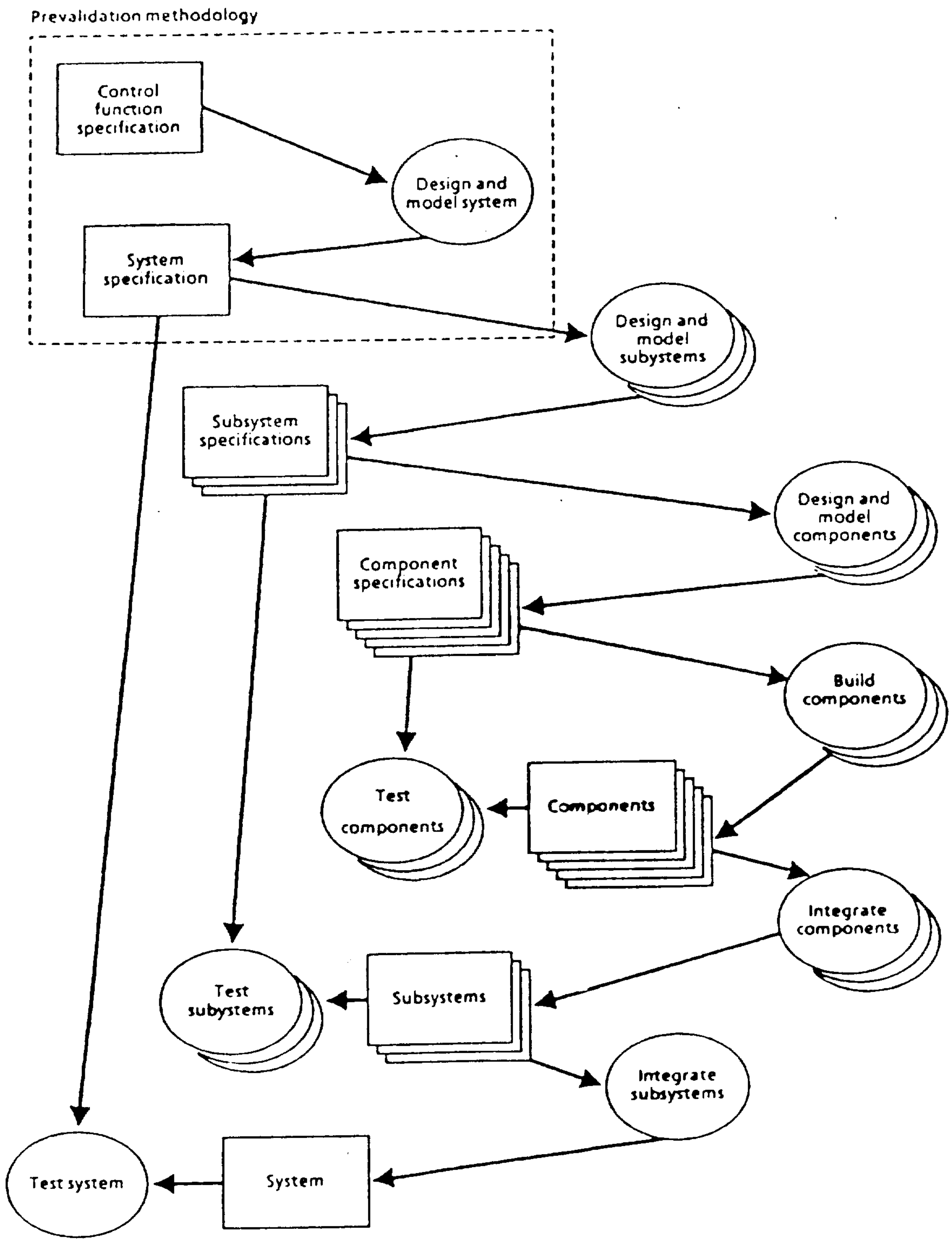
IAPSA II Prevalidation Methodology



Prevalidation Methodology

- Early evaluation exposes system weaknesses
- Reliability and performance analysis versus staffing level unresolved
- Methodology allows assessment of cost and technical risk
- Seems to mirror Japanese staffing concept





Design and Validation Phases

Building-Block Considerations
Contractor/Subcontractor Relationships

- Requires different approach to subcontractors
- Need to develop:
  - Functional specification
  - Reliability attributes
  - Performance attributes
- Requirements only will not suffice
- Subtleties of building-block interrelationships important

Building-Block Considerations
Contractor/Subcontractor Relationships (continued)

- Enforcement of rigor on the vendors
- Do we need a two-step procedure with vendors—
  - During building-block definition
  - During hardware/software bid on system

Methodology

Incomplete

- Additional tools
  - Maintainability
  - Availability
  - Survivability
  - Cost
- Software
  - Tie in to top-level system design
- Relationship between full nonlinear simulation and performance model
- Hardware and software build—subsystem validation and verification
- Lab testing
- Flight testing

Tools

Major effort on

- Model development—candidate architecture definition
  - How system works
  - Brief, concise, easy to generate
  - Must include redundancy management operation
- Output data interpretation
  - Complex
  - Very time consuming

Performance Modeling

- Difficult to simulate
  - Conceptual problem
  - Difficult to implement
    —I/O system service
- Detail of simulation is based upon judgement
- Simulation can validate system architecture
- Verification of model with architecture description
- Simulation used through life cycle
- Unexpected insight via performance simulation

Reliability Modeling

Methodology goal: rapid evaluation of architecture alternatives

- Current evaluation cycle too slow
- Tools available for ultrareliable systems
  - Short-duration safety
- Long-duration reliability also important
  - Operation with failures
- Common evaluation tool and similar models (safety, mission, etc.) desirable (mandatory?)
- Level of detail and model simplification currently an art
  - Strong pressure toward small and simple models
  - ASSIST/SURE supports techniques for short-duration problems (long-duration?)

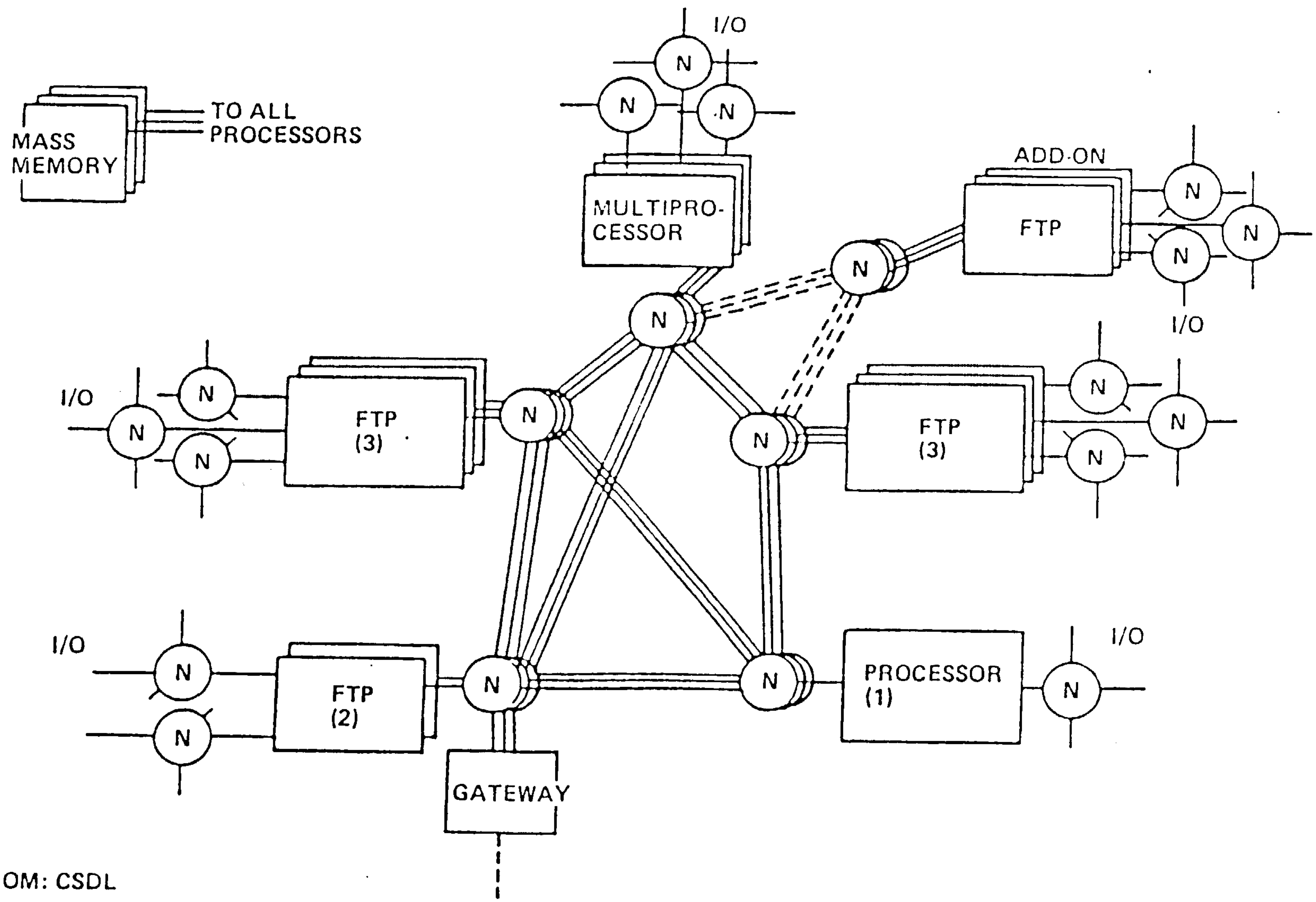
Advanced Information Processing System

(AIPS)

Designed
By

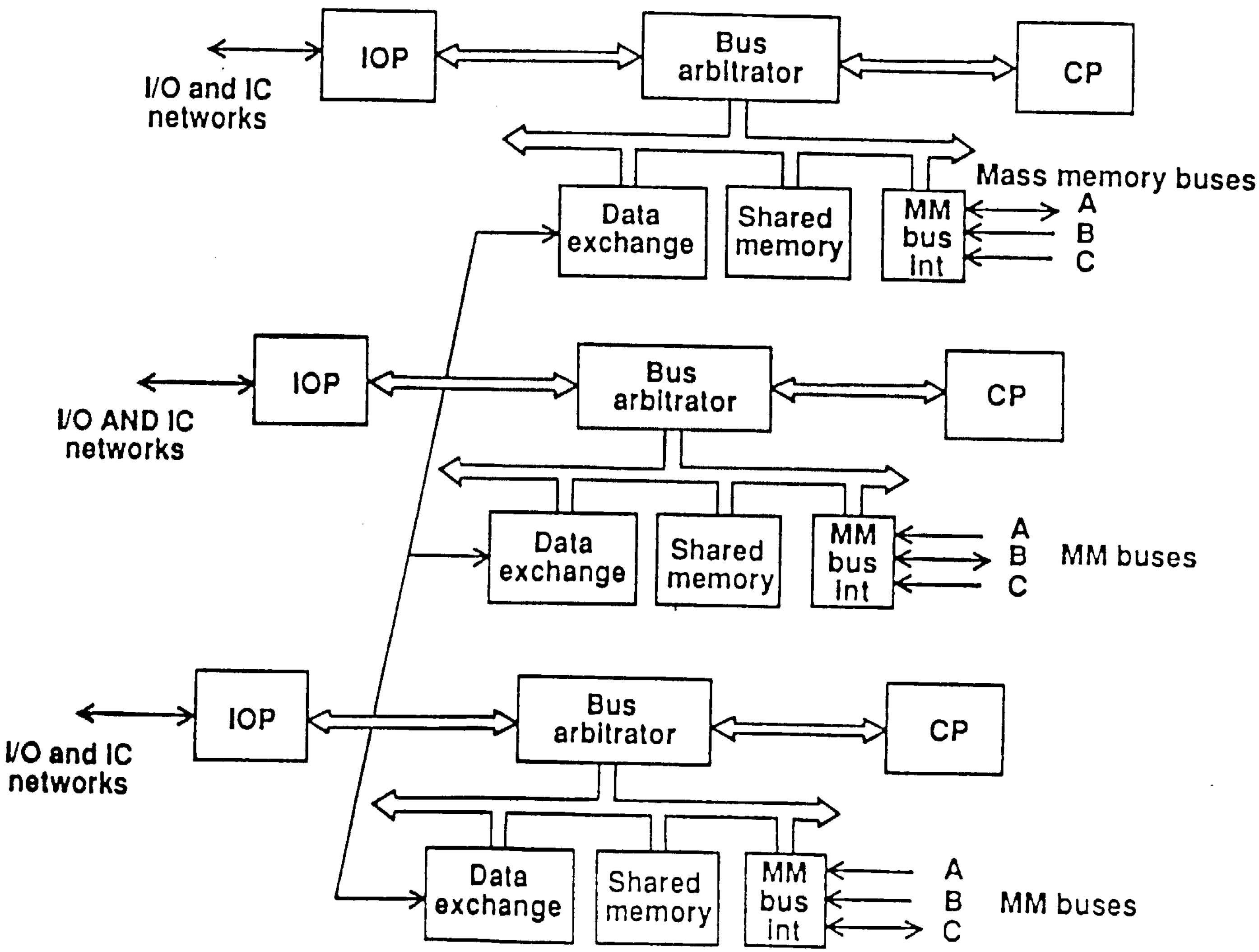
Charles Stark Draper Laboratory

AIPS Proof-of-Concept Configuration

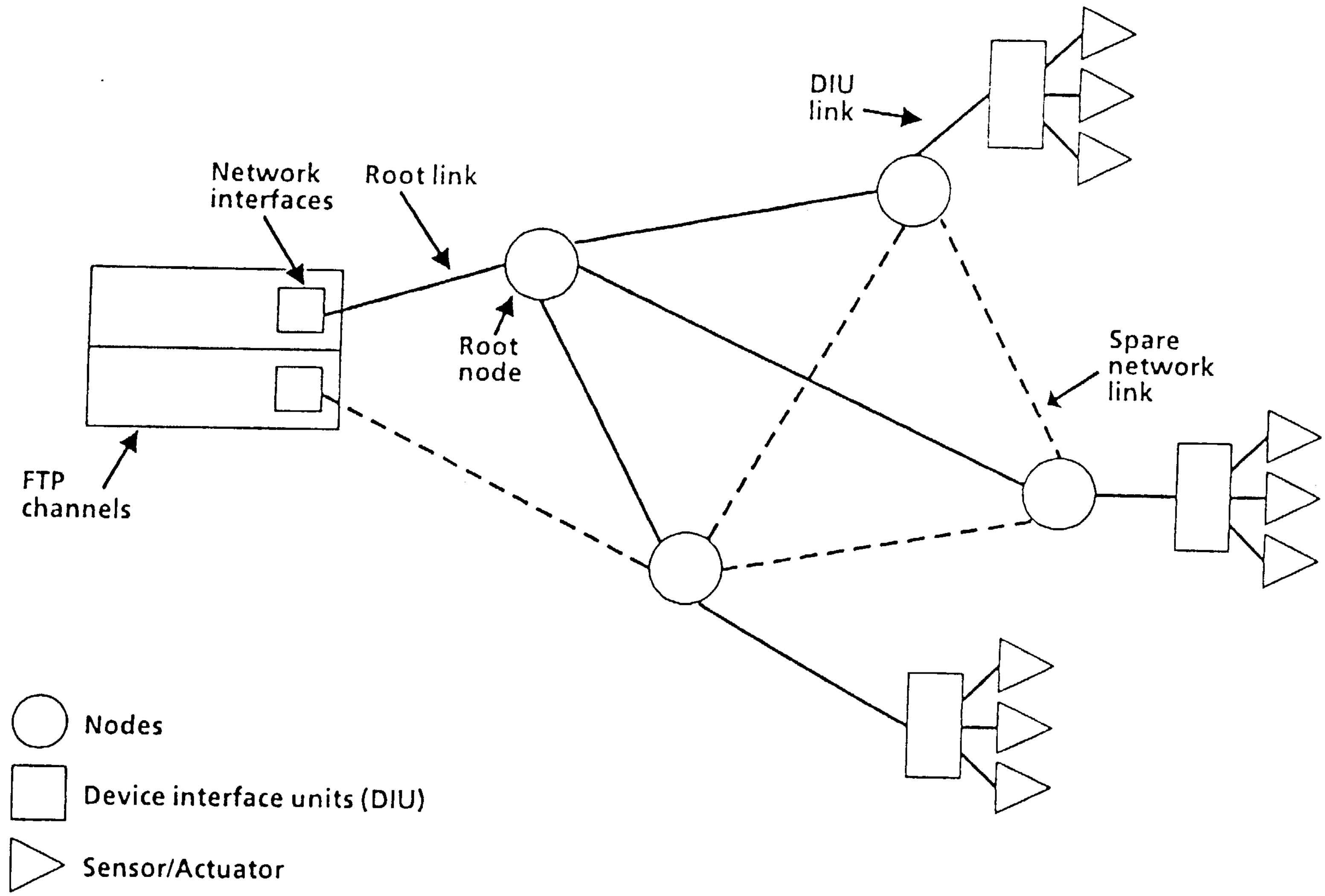


FROM: CSDL

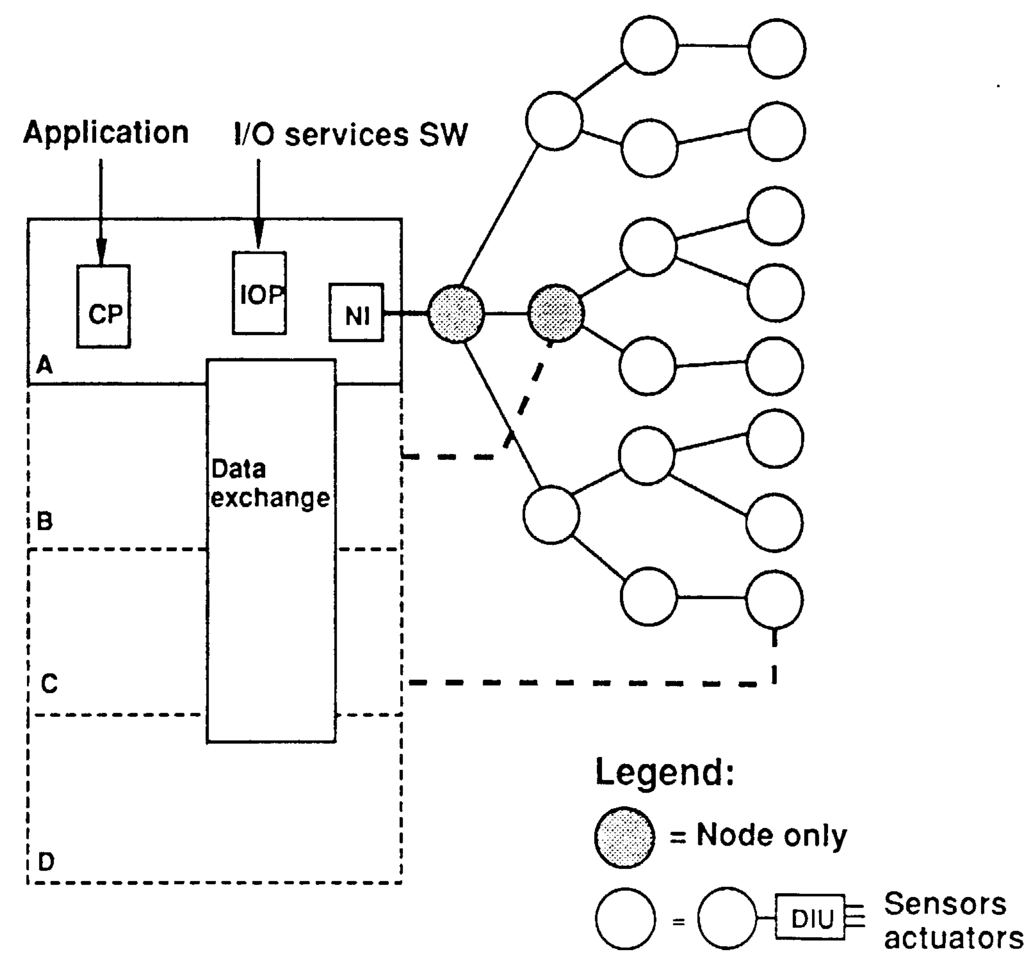
FTP HW And SW Provide Failure Protection



I/O Network Elements

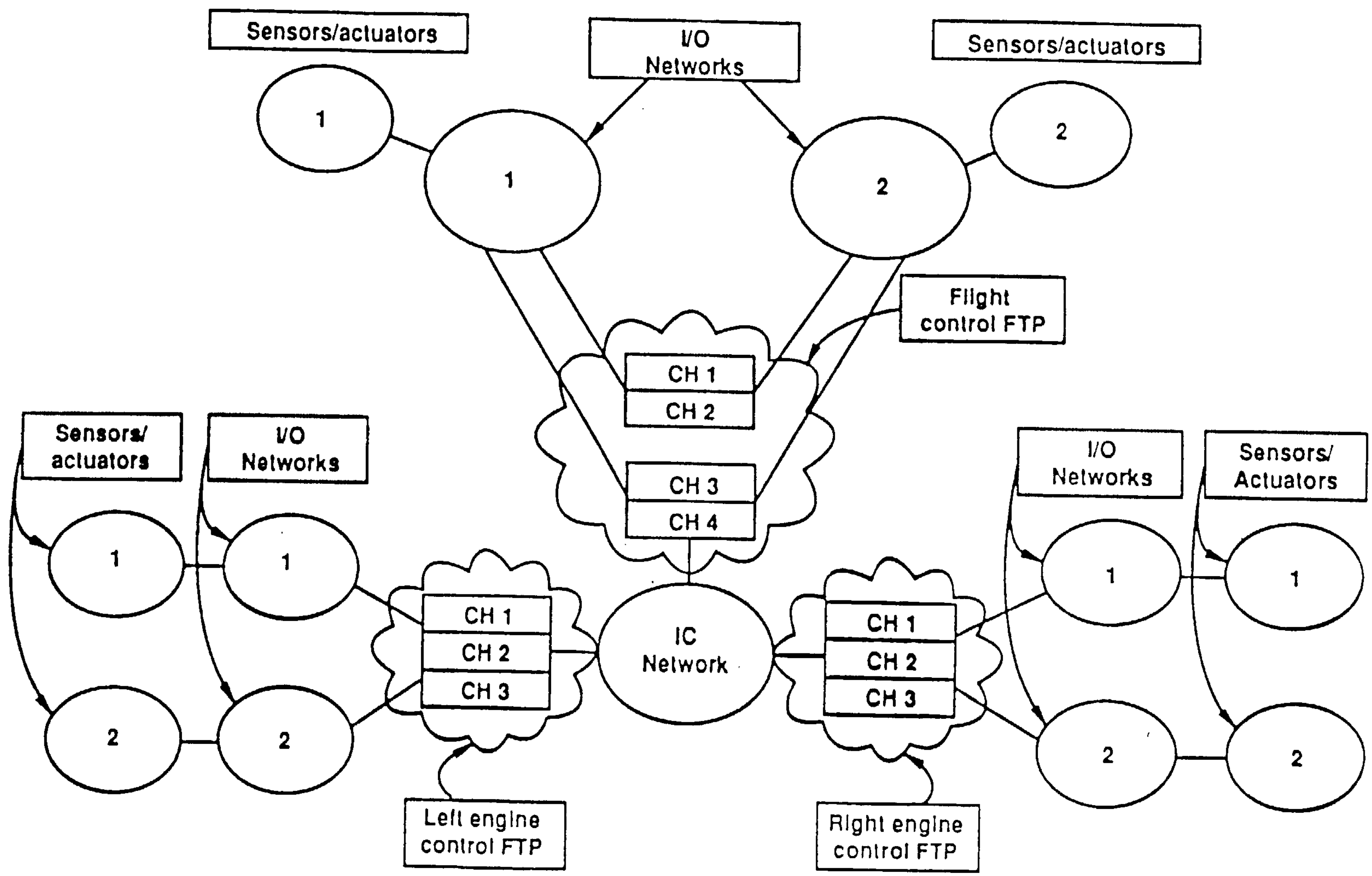


Flight Control Computer With I/O Connections



Architecture

Reference Configuration Overview



C8158-04.001-L7130 D4 ai

Testing Experience

- Application was quickly integrated into complex fault-tolerant AIPS system
  - AIPS simplex application programming model
  - CSDL staff assistance
- Impossible to meet goal of testing system with real time performance demands
  - Slow time testing focused on system level interactions
- Nonintrusive measurements likely requirement for validation
  - During real-time operation with full workload
  - System services or operating system functions critical
  - Not provided for in original AIPS testing/validation concept

General Observations
Architecture

AIPS

General Observations

Architecture

- Integrated flight control/propulsion control—feasible
  - Obstacles—mind set problem
- Minimum use of sensors/activators
- Allows for optimum control
- Allows for function migration
- Growth potential
- Subset of Vehicle Management System

General Observations (Cont)
AIPS

Very innovative for its time
- Supports true distributed system
- System redundancy transparent to user
- General set of building blocks—user selected
- Fault containment regions

General Observations (Cont)

AIPS

- Advantages
  - Building blocks allow expansion with minimum change
  - Building block concept supports common hardware/software throughout the airplane
  - Prevalidated building blocks for both hardware and software
  - Ability to mix elements with different reliability requirements
  - Distributed computing possible
  - Function migration possible
  - Minimizes maintenance and logistic issues

General Observations (Cont)

AIPS

- Advantages (cont)
  - System redundancy is inherent in AIPS design
  - Fault containment region is inherent in AIPS design
  - Pre-emptive priority allows application flexibility
  - Communications protocol allows design for minimum sensor/actuator time skew
  - Concept supports dispatch with failures (need faster network repair time)
  - Variation of components within FTP channel (CP/IOP or CP)

General Observations (Cont)
AIPS

- Concepts needing attention
  - Insufficient documentation
  - IOP/Data Exchange bottleneck
  - IC network traffic uncertain (not modeled)
  - No discernable difference between network and bus for IAPSA requirements

General Observations (Cont)

AIPS

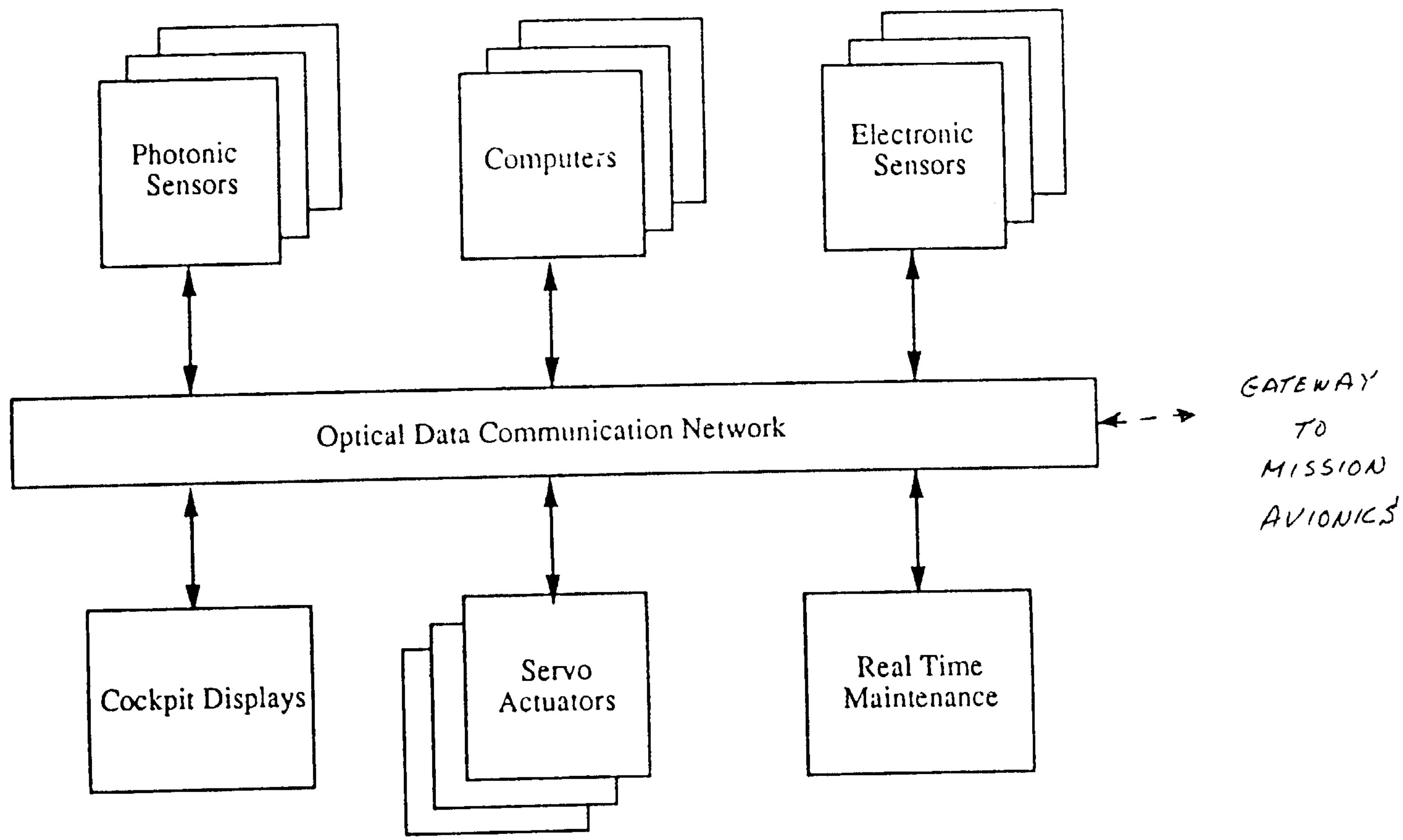
- Concepts needing attention (cont)
  - Complex validation issues
    - —IO system services
    - —IC system services
    - —Pre-emptive priority scheduling
  - Resynchronization of channel during flight not possible with present design
  - System design guidelines not established
  - If IC modeled—it appears system would not work with present timing and loading requirements

Future Systems

Vehicle Management System

- All flight critical functions
  - Failure causes loss of aircraft

- Near term - military
- Long term - commercial



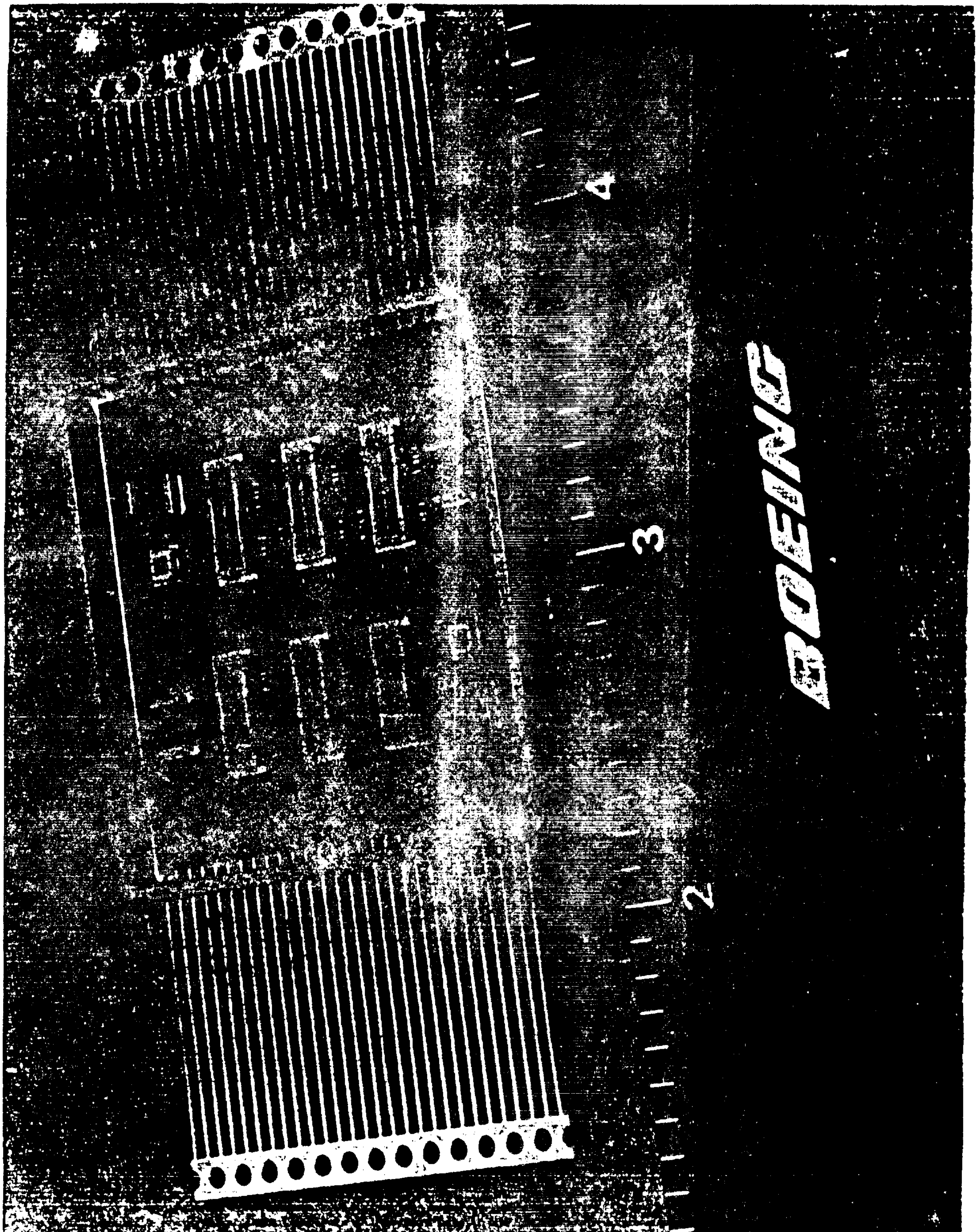
Generic VMS Architecture

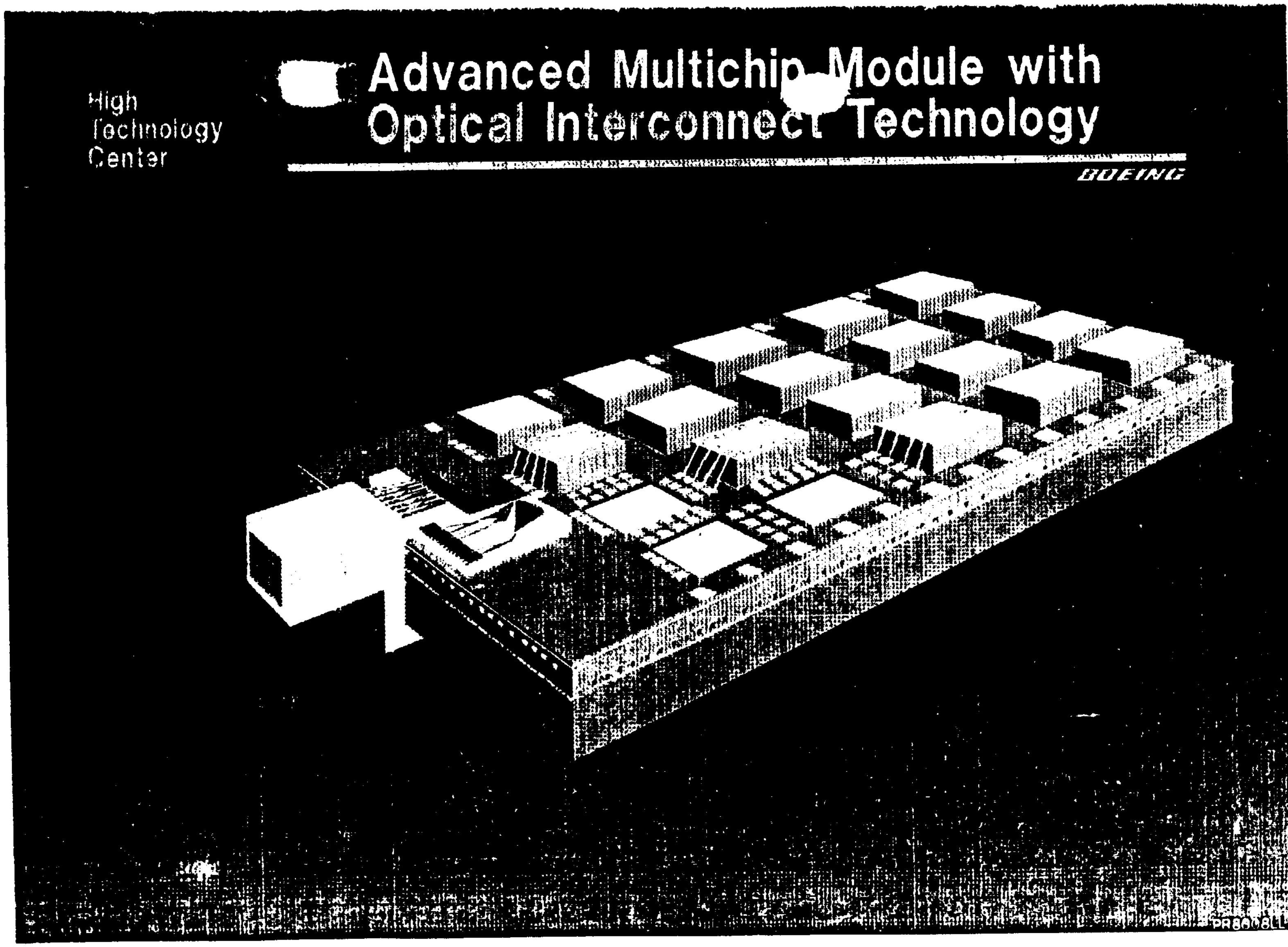
Photonics used for

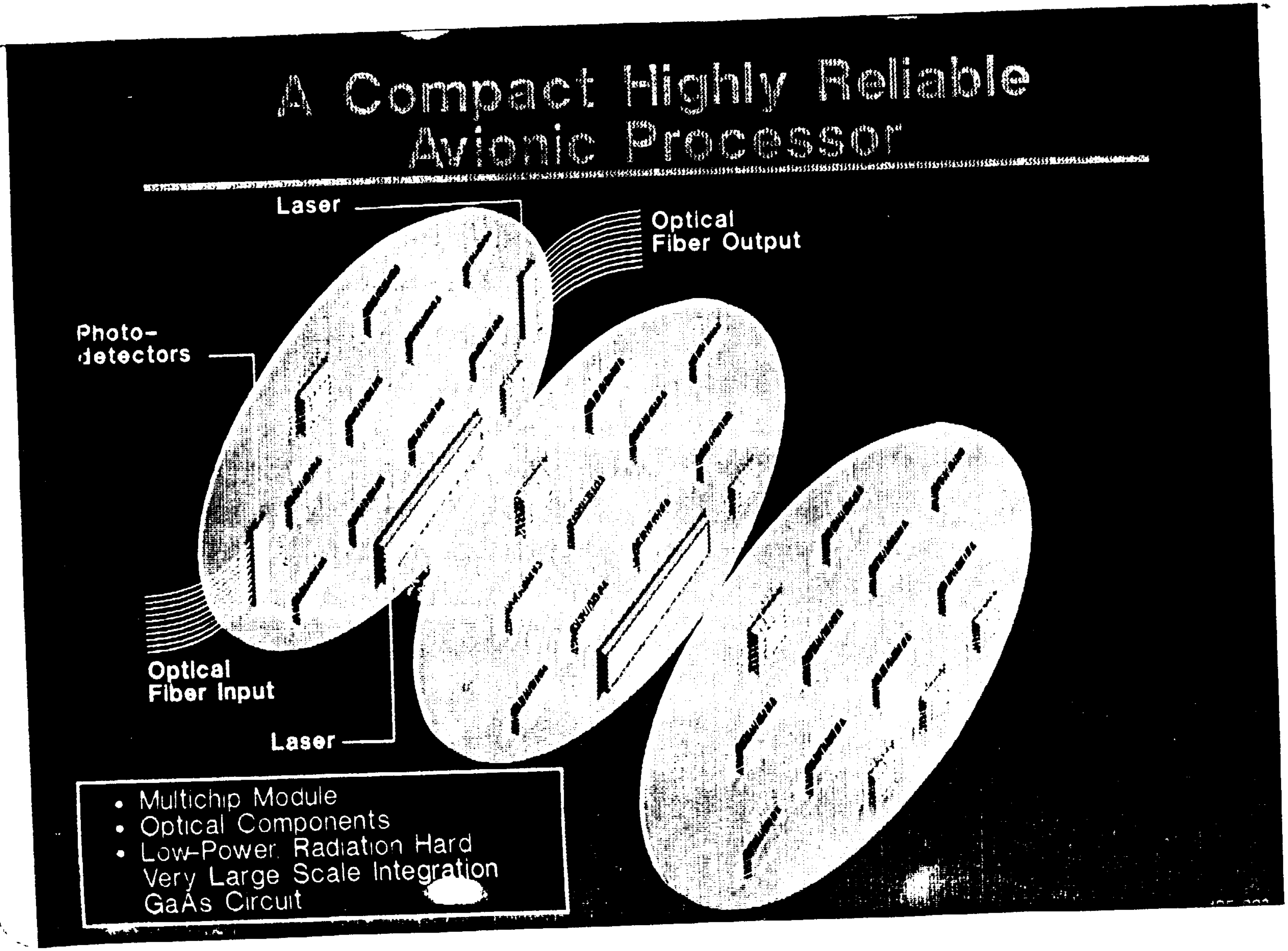
- Bus
- Sensors
- I/O
- Actuators
- Computers (20 years)

Benefits of VMS

- Performance
  - Unified environment - coordination of all tasks
- Growth capability
  - Additional nodes - minimum impact
  - Life cycle replacement - minimum topology impact
- Reliability
  - Minimum set of building blocks
  - Minimum part count
  - Common I/O
  - Sharing of sensor data
  - Common redundancy management


BOEING
2
3
4


High
Technology
Center
Advanced Multichip Module with
Optical Interconnect Technology
BOEING
PR8008LL


A Compact Highly Reliable
Avionic Processor
Laser
Optical
Fiber Output
Photo-
detectors
Optical
Fiber Input
Laser
• Multichip Module
• Optical Components
• Low-Power, Radiation Hard
Very Large Scale Integration
GaAs Circuit

What does all this mean in terms of validation and verification?

- Design for validation is a critical technology
- Need indepth V&V concurrent with design analysis

Solution to V&V

Formal Verification - viable solution to the V&V problem for

- Requirements/Specifications
- Hardware
- Software
- System

Where are we in Formal Verification?

- the following 3 days should tell us!!