# Modular Avionics for the New Space Vision: The JPL Perspective

Gary Bolotin
NASA – JPL
gary.s.bolotin@jpl.nasa.gov

# Agenda

- What are the challenges?
- Development of multi-purpose, re-configurable modular building blocks
- Development of adaptable re-configurable architectures for long-life, high reliability, and mission adaptation
- Key Future Challenges
  - Partitioning and the Orthogonalization of Tasks
  - Sharing and Isolation
  - Fault Tolerance
  - Fault tolerance, COTS, and rad-hard parts
  - Autonomous System Recovery Functions
- Conclusion: How JPL will address the challenge

# What Are the Challenges?

- Standard Interfaces
- Development of multi-purpose, re-configurable modular building blocks
- Development of adaptable, autonomously re-configurable architectures for long-life, high reliability, and mission adaptation

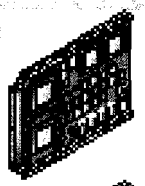
# Industry Standard Interfaces

- cPCI
- IEEE 1394
- I2C
- 802.11

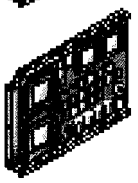
# Multi-purpose, re-configurable modular building blocks

- X2000 Avionics & Power Electronics
- Architecture Platform Electronics
- Mobility Avionics: A Re-configurable Building Block

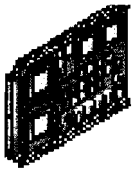
# X2000 Avionics Hardware Building Blocks



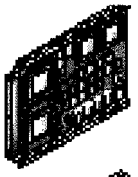
**SFC—System Flight Computer**
- Power PC 750 compact peripheral component interconnect (CPCI)–based
- 128 Mbytes DRAM; 256 kbytes EEPROM
- Baseline 240 MIPs; variable speed
- Contractor: BAE Systems



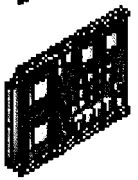
**SIO—System Input/Output**
- Peripheral component interconnect (PCI) 1394/I²C bridge; 2 universal asynchronous receiver/transmitters (UARTs)
- Includes node reset control; general fault protection logic; discretes
- Assembly developed by JPL



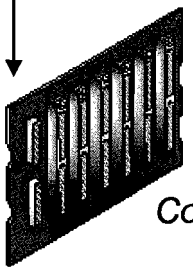
**NVM—Nonvolatile Memory**
- 2 Gbits/slice Flash Memory
- Includes power management control and erase/write cycle tally
- Contractor: SEAKR Engineering, Inc.



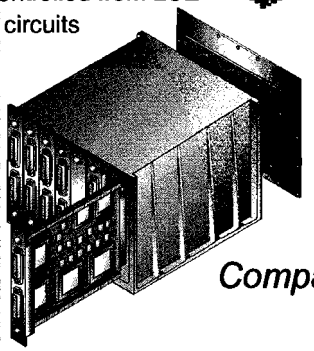
**SIA—System Interface Assembly**
- Includes 1553, SPI, and high-speed serial interfaces
- Assembly developed by JPL



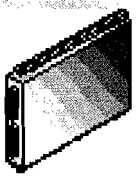
**TIF—T Zero (Tz) Interface**
- Contains critical safety relays controlled from LCE
- T Zero-launch vehicle interface circuits
- Assembly developed by JPL



*Compact PCI Backplane*

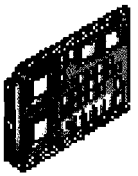


*Compact PCI Chassis*

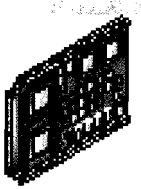


**PCA—Power Converter Assembly**
- Two 30-W primary-to-secondary power converter modules (PCMs) on 1 slice
- Two versions: dual 3.3-V PCMs or one 3.3-V PCM and one 5-V PCM
- Contractor: Lockheed Martin Commercial Space Systems (CSS)

**PSS—Power Switch Slice**
- Used to switch power loads, valves, and pyros (all three functions)
- 16 switches/slice
- Redundant I²C bus
- Contractor: Lockheed Martin CSS

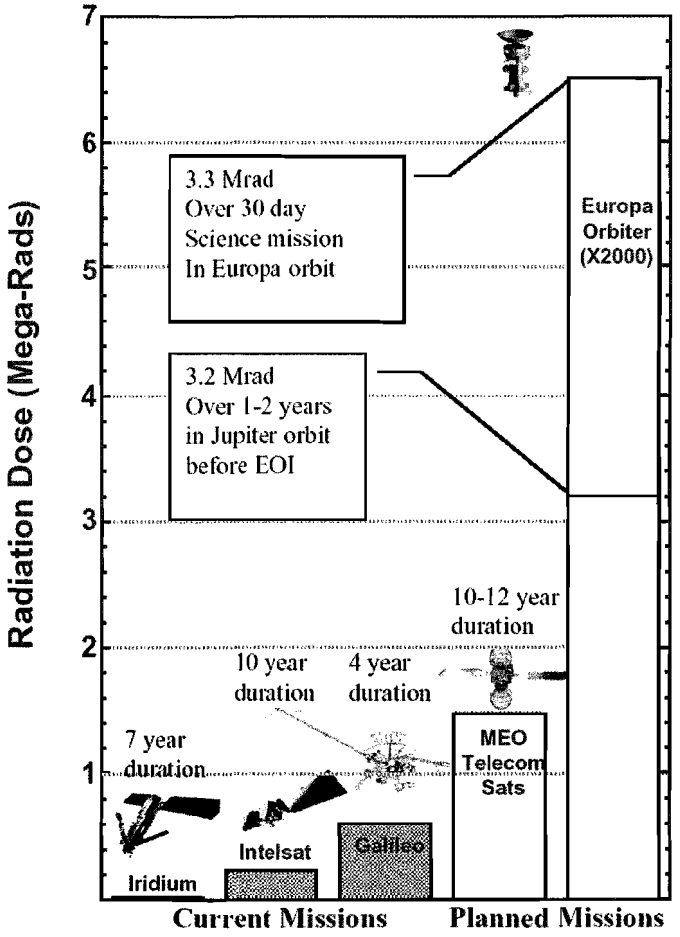


**PCS—Power Control Slice**
- Primary spacecraft power bus regulation
- Includes shunt regulator control
- Redundant I²C bus
- Contractor: Lockheed Martin CSS

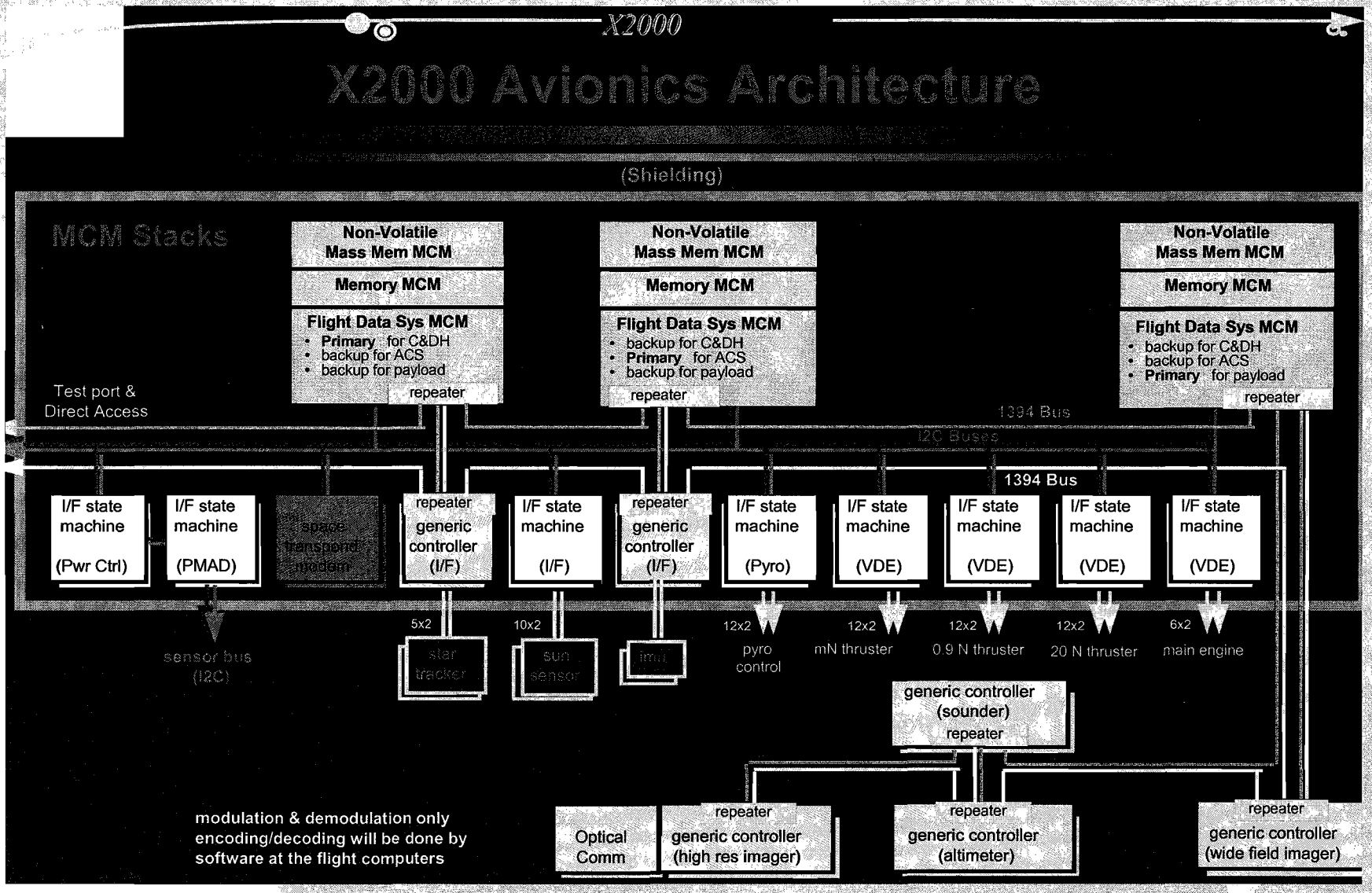


**TAS—TRIO Assembly Slice**
- Temperature and analog collection
- 6 Temperature remote I/O (TRIO) application-specific integrated circuits (ASICs) split between two I²C buses
- 96 Telemetry channels; 10-bit A/D
- Contractor: Johns Hopkins University, Applied Physics Laboratory

# X2000 Avionics Hardware Building Blocks

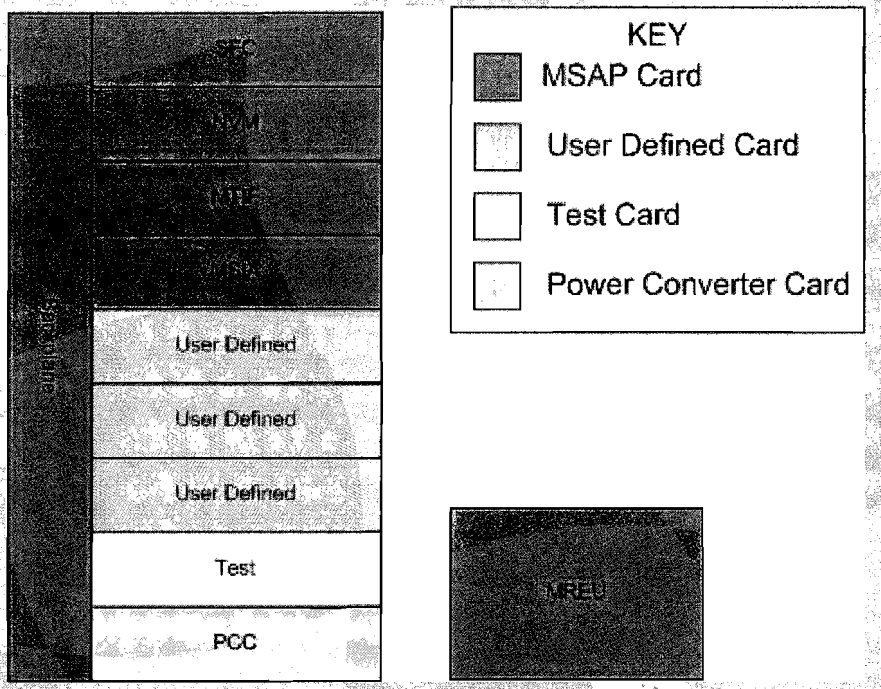



- The Europa Orbiter total dose environment is harsh compared to current experience
  - At Europa an astronaut inside an EVA suit receives a lethal dose every 12 minutes
- The Europa Orbiter must operate with high reliability during the 30 day mission
  - Science objectives
  - Achieve quarantine orbit
- Impact
  - High technology, high risk, high cost electronics development (X2000) to reduce risk
  - Total shielding = 39 kg

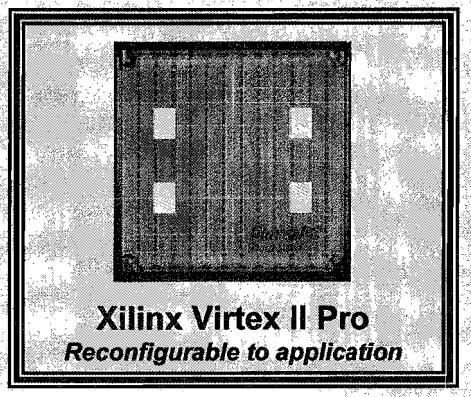

X2000
X2000 Avionics Architecture
(Shielding)
MCM Stacks
Non-Volatile Mass Mem MCM
Memory MCM
Flight Data Sys MCM
• Primary for C&DH
• backup for ACS
• backup for payload
repeater
Non-Volatile Mass Mem MCM
Memory MCM
Flight Data Sys MCM
• backup for C&DH
• Primary for ACS
• backup for payload
repeater
Non-Volatile Mass Mem MCM
Memory MCM
Flight Data Sys MCM
• backup for C&DH
• backup for ACS
• Primary for payload
repeater
Test port & Direct Access
1394 Bus
I2C Buses
1394 Bus
I/F state machine (Pwr Ctrl)
I/F state machine (PMAD)
space transponder modem
repeater generic controller (I/F)
I/F state machine (I/F)
repeater generic controller (I/F)
I/F state machine (Pyro)
I/F state machine (VDE)
I/F state machine (VDE)
I/F state machine (VDE)
I/F state machine (VDE)
sensor bus (I2C)
5x2
star tracker
10x2
sun sensor
imu
12x2
pyro control
12x2
mN thruster
12x2
0.9 N thruster
12x2
20 N thruster
6x2
main engine
generic controller (sounder)
repeater
modulation & demodulation only
encoding/decoding will be done by
software at the flight computers
Optical Comm
repeater
generic controller (high res imager)
repeater
generic controller (altimeter)
repeater
generic controller (wide field imager)

# JPL Multi-Mission Architecture Platform

- Jet Propulsion Laboratory's Multi Mission System Architectural Platform (MSAP) project is a program designed to provide JPL missions with a standard set of hardware and software components that can be adapted and customized to fit mission-specific needs



## Xilinix Virtex II Pro Qualification & SEU Mitigation Methods



**Xilinx Virtex II Pro**
***Reconfigurable to application***

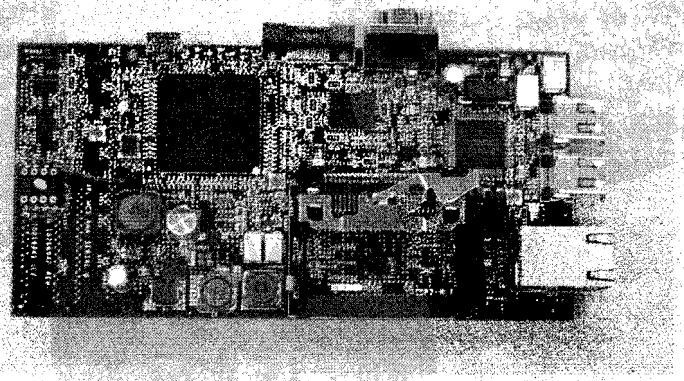
## Resources we bring to the Table

- JPL is a founding member of the Industry consortium aimed at space qualification of Xilinx devices This consortium has consolidated efforts of many aerospace organizations and to take advantage of the several competencies of its members to evaluate Xilinx FPGAs
- JPL is funded to address the qualification tools and methods for using the Xilinx Virtex-II Pro, Virtex 4, and later, the Virtex 5 devices for flight applications

Description of past accomplishments

- JPL has qualified the use of Xilinx Virtex devices for use on MER
- JPL has qualified the future use of Xilinx Virtex II devices
- JPL has developed SEU mitigation methods for the Xilinx Virtex II Pro
- For more information:
  http://kevin.org/Watson_MSMT-2004_Proposal.pdf

## Mobility Avionics: A reconfigurable Avionics Module




*First Prototype Module*

## Resources we bring to the Table

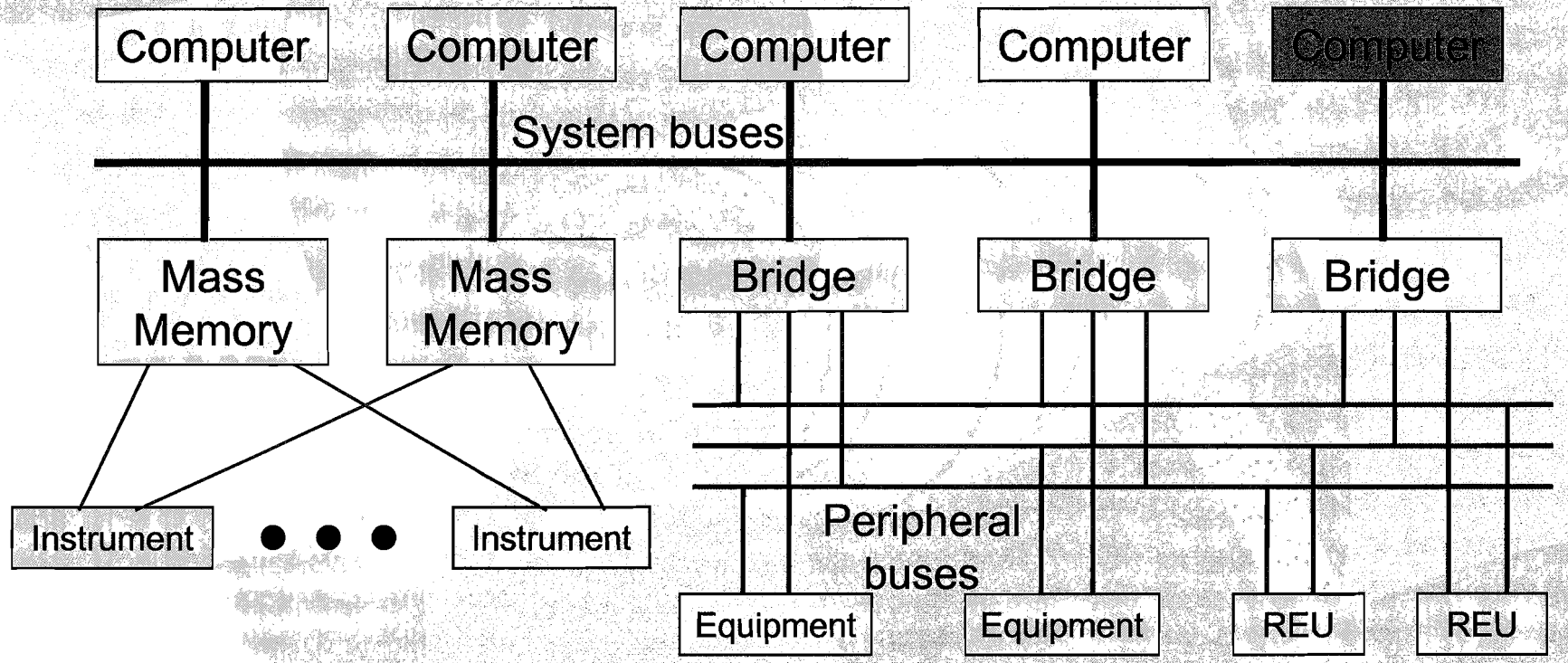
- JPL has developed a reconfigurable avionics module that is a complete avionics subsystem capable of supporting surface mobility tasks at the state-of-the-art RAD750 performance level with over a 10x reduction in system power demand, mass and volume for moderate radiation missions.
- This module can be used alone for a small avionics system or used in a network as a building block for future avionics systems.
- JPL has worked closely with Xilinx, Monta Vista, in developing this product

Description of past accomplishments

- Flight Qualifiable design
- Working Prototype Module
- Successful Alpha source testing of SEU mitigation methods
- Porting of JPL Stereo and CLARATY code base

- For more information:
  http://rtd/reports/rtd04/pdfs/R03009021.pdf

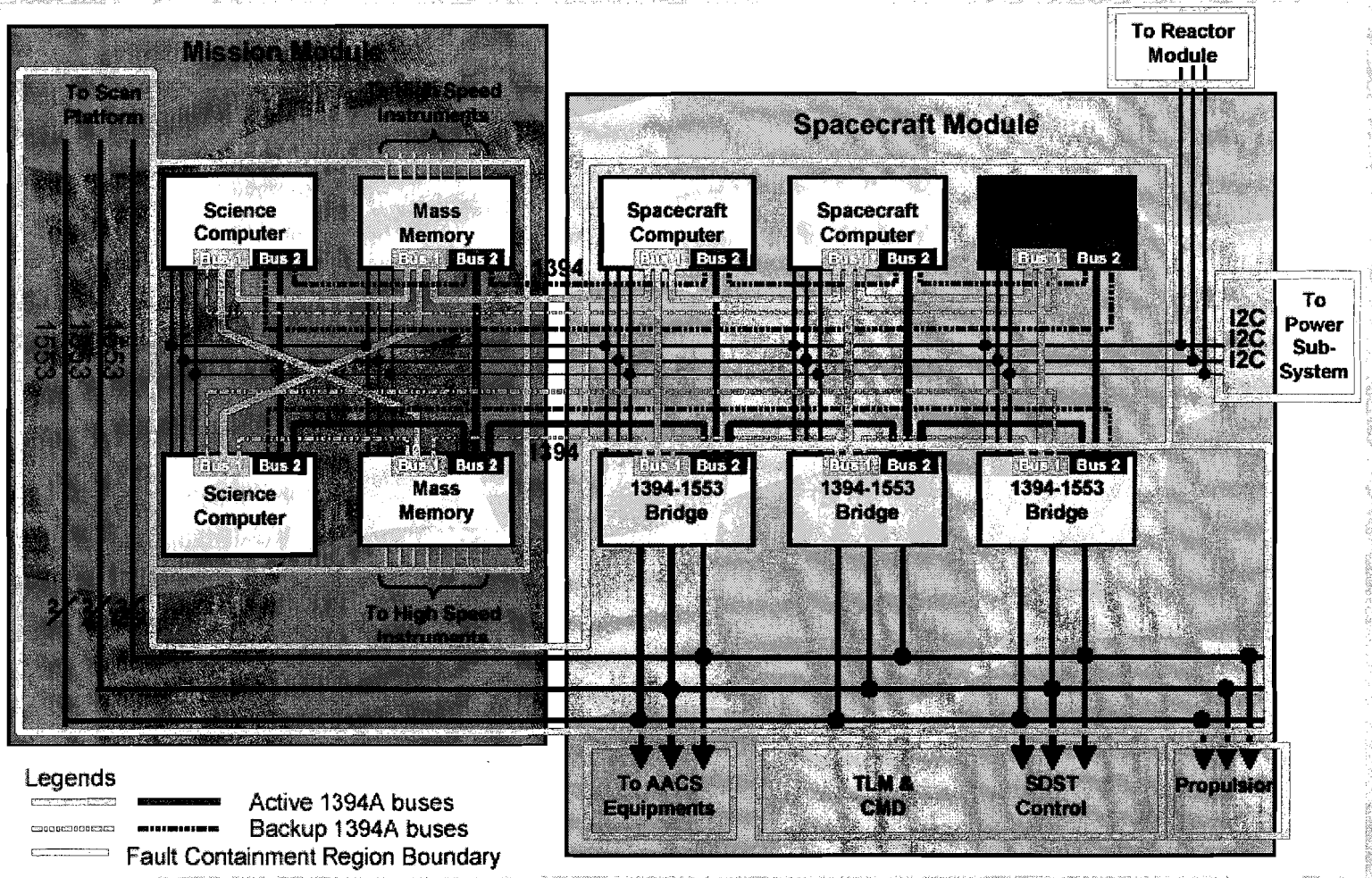
# Design Concept



# JIMO CDH Design Approach

- The Symmetric architecture
  - All computers are identical, and their roles can be configured easily
  - The high-speed system bus connects all nodes
    - Computers
    - Mass Memories
    - Bridges
  - The peripheral bus connects the C&DH to other subsystems equipments
  - Bridges connect the system bus with the peripheral bus
  - All computers have the same access to all MMs, equipments, sensors, and actuators
- The Advantages
  - Flexible and scalable

# JIMO CDH Hardware Architecture



# C&DH Fault Tolerance Approach

- Fault Containment
  - Capture heterogeneity of fault tolerance by the concept of *Fault Containment Region*

| Fault Containment Region | Fault Tolerance Level |
|---|---|
| **Spacecraft Module C&DH** | **2** |
| **Mission Module C&DH** | **1** |
| **Science** | **0** |
| **AACS** | **2** |
| **Telecom** | **1** |
| **PC&D** | **2** |
| **Thermal Management** | **1** |
| **Electric Propulsion** | **1/2** |
| **Reactor Module Control** | **2** |
| **Reactor** | **1** |

# Partitioning and the Orthogonalization of Tasks

- How does one best split up such a system into semiautonomous functions housed in different modules with carefully designed and fully understood interfaces? First it is necessary to choose an intercommunication approach that is not only exceptionally reliable, but will be consistent with standards over the next several decades. A highly redundant and damage tolerant (physically distributed) switching fabric is our recommended approach. Next, we propose to extend "plug and play" technology to unique CEV and space needs. This involves developing standard but extensible functional interfaces (for commands, timing, data) for various subsystem types that in effect creates a "virtual subsystem." The virtual subsystem hides many of the complexities inside and provides an interface that simplifies system integration and test, guarantees hard real-time performance to functions that need it, and it supports the necessary redundancy, self-test, fault-tolerance and autonomy needed for a dependable system. This approach is necessary so that functions can be changed or hardware/software replaced without complicating and compromising the dependability of the rest of the system. Stated simply, changing or adding a function or module should not require re-validation of others that are not directly related.

# Sharing and Isolation

- *Physical sharing* Whenever different functions share physical resources such as interconnection buses, shared memory and processor resources, some must wait for others – even if they do not interact in any other way. Sufficient bandwidth and a careful system-level timing (and intercommunications) strategy will be provided so that plugging in or changing system modules and functions will not affect the real-time performance of unrelated functions.
- *Information sharing* by processes that interact and their impact on real-time applications must be thoroughly understood. Perhaps the best approach here will be to develop a directed graph based analysis tool that insures correct data is produced in a timely fashion, and that can be used iteratively during the design process.
- *Isolation of some highly protected (e.g. life critical) functions* will be necessary either by use of firewalls or possibly by disconnection from other parts of the system.

# Fault Tolerance

- Fault-Tolerance is the process by which the on-board computers detect and recover from errors and faults. The flight-critical parts of the system will require extremely high reliability and even tolerance to localized physical damage, not unlike modern commercial aircraft. Unlike an airliner that lands within 15 hours, the CEV must maintain its high reliability for months. Massively redundant fault-tolerance techniques currently employed for commercial aircraft will be further developed and expanded upon, including design diversity in hardware and software to prevent design errors or undetected fabrication flaws from causing system failure. The ability to include additional redundancy will be included to extend the reliable life of the CEV system. For less critical high performance processing requirements (for which checkpointing and rollback are acceptable) can be implemented in a fashion that uses less redundancy and thus makes more resources available to increase computing performance. JPL and its contractors have developed architectures and techniques for doing this that are at TRL 4.

# Fault tolerance, COTS, and rad-hard parts

- In order to achieve acceptable performance, to have available modern software development tools, and to be able to use standards that are amenable to system evolution over time, complex components (processors, memories, etc.) will be implemented with COTS parts whenever possible. Fault-tolerance techniques have been demonstrated at JPL and by others allow dependable performance in the presence of Single Event Upsets. Small rad-hardened glue chips also will be needed to provide simple "hard core" functions, such as performing final output voting to prevent spurious errors from reaching actuators, performing simple embedded control functions, or implementing state machines to initiate restarts upon detecting system failure.

# Autonomous System Recovery Functions

- Given that a dependable computing capability is achieved, then Autonomy software can be used to detect failures in their host electromechanical subsystems and take system level actions to compensate for fault conditions. Creating virtual subsystems with built-in self test capability (1 above) both facilitates system integration and also is a major aid to the autonomous recovery process. Autonomous recovery consists of determining what spacecraft functions are not working properly, substituting spares when possible to resume nominal operation, or determining alternate spacecraft operating modes upon loss of resources. It also includes modifying commands and operations to accommodate for time outages when a repair has been attempted. JPL has been a leader in developing this capability

# Conclusion

- What are the challenges?
- Development of multi-purpose, re-configurable modular building blocks
- Development of adaptable re-configurable architectures for long-life, high reliability, and mission adaptation
- Key Future Challenges
  - Partitioning and the Orthogonalization of Tasks
  - Sharing and Isolation
  - Fault Tolerance
  - Fault tolerance, COTS, and rad-hard parts
  - Autonomous System Recovery Functions
- Conclusion: How JPL will address the challenge