SAE Aerospace
An SAE International Group

Shuttle Architecture and Identical Inputs

Christopher Scott Cox

August 23, 2007

USA
United Space Alliance

Brief History

- A total of 6 orbiters were constructed named Challenger, Columbia, Enterprise, Endeavor, Atlantis, and Discovery
  - Enterprise was used for approach and landing test and for some early Pad testing
  - Of these six, three are currently in the fleet (Endeavor, Atlantis, and Discovery)
- The program just completed the 119th Shuttle Flight (STS-118) with the return of Endeavor in August 2007
  - This was Endeavor's first flight after a major refit
  - STS-118 was the first flight where a 3 string GPS configuration was used for entry
  - This flight was the 22nd flight to the International Space Station which now consists of 6 habitable modules
- With the completion of Endeavor's refit, each shuttle in the fleet now contains a glass cockpit consisting of a total of 11 Multifunction Display Units (MDU)

Information and Photos courtesy of NASA

Architectural Concerns

- Significant architectural considerations:
  - Reliability and fault tolerance
    - FO/FS (Fail Operational/Fail Safe)
  - Flight control critical timing requirements
    - For example:

    Input / Compute / Output (Flight critical transport lag = 18 ms)

    (E.G. Rotational Hand Controller (RHC) , Rate Gyro Assembly (RGA), Angular Accelerometer (AA) Inputs / Compute / Aerosurface Output)
  - Computer memory limitations
    - Mass Memory Unit (MMU): 16 MB
    - General Purpose Computer (GPC) Main Memory: 1 MB
      - Initial design had 64K Fullwords (FW) (256 KB)
      - AP-101B Flight GPCs had 104K FW

Reliability

- Reliability is the overriding criterion for computers and software

- Reliability and fault tolerance achieved thru redundancy to meet FO/FS Requirement
  - Fail Operational: Remain fully operational after a single failure of any subsystem
  - Fail Safe: Remain safe even after two failures of the same subsystem

- Four redundant GPCs required to provide tolerance to the failure of 2 GPCs (5^{TH} GPC reserved for redundant software System – Backup Flight System (BFS))
  - 1^{ST} Primary Avionics Software System (PASS) GPC failure reduces voting group to 3 members
  - 2 of 3 voting logic to identify 2^{nd} failed PASS GPC

Reliability (cont.)

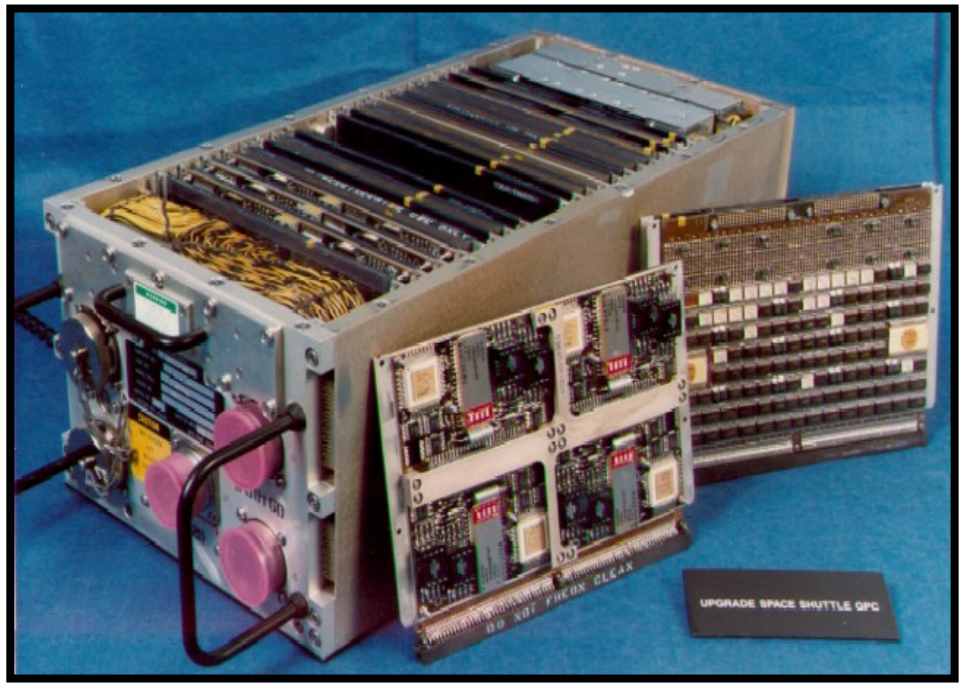
- The synchronized redundant set architecture of the Space Shuttle DPS was chosen in preference to independent channel or master/slave alternatives based on trade-offs of the following requirements and concerns:
  - Allowable downtime during dynamic flight phases for failure recovery
  - Fault tolerance requirement (FO/FS)
  - Time correlation and tolerance limits for commands to flight control actuators, Main Engine Controllers (MECs), Engine Interface Units (EIUs)
    - I/O Skews, Jitter, Transport Lag, etc.
  - Susceptibility to database pollution from a faulty GPC
  - Susceptibility to failure modes that allow a faulty computer to assume increased control authority
    - No Automatic Bus Reconfigurations

Identical Inputs give Identical Outputs

- The basic premise of the shuttle redundant set operation is that identical computers receiving identical inputs and executing identical instruction sequences will compute identical outputs. This premise and identified system requirements drive the synchronization requirements.
  - All GPCs must receive identical inputs, and data from redundant sensors must be time correlated so values can be meaningfully compared (e.g. 3 Inertial Measurement Units (IMUs), 4 Air Data Transducer Assembly (ADTAs), 4 AAs, 4 RGAs)
  - All GPCs must accept or reject the same subset of redundant inputs
    - Use of Sync Codes + I/O Problem Report (IPR) ICC to agree on success / failure of I/O
  - All GPCs must use identical data for computations and decisions
    - Selection Filter Logic (e.g. Mid-Value Select for redundant sensor data such as IMU, RGA, AA, etc.)
  - All GPCs must output flight control actuator commands within time correlation and tolerance limits
  - Failed GPCs must be detected and isolated without affecting the performance of the remaining set

GPC

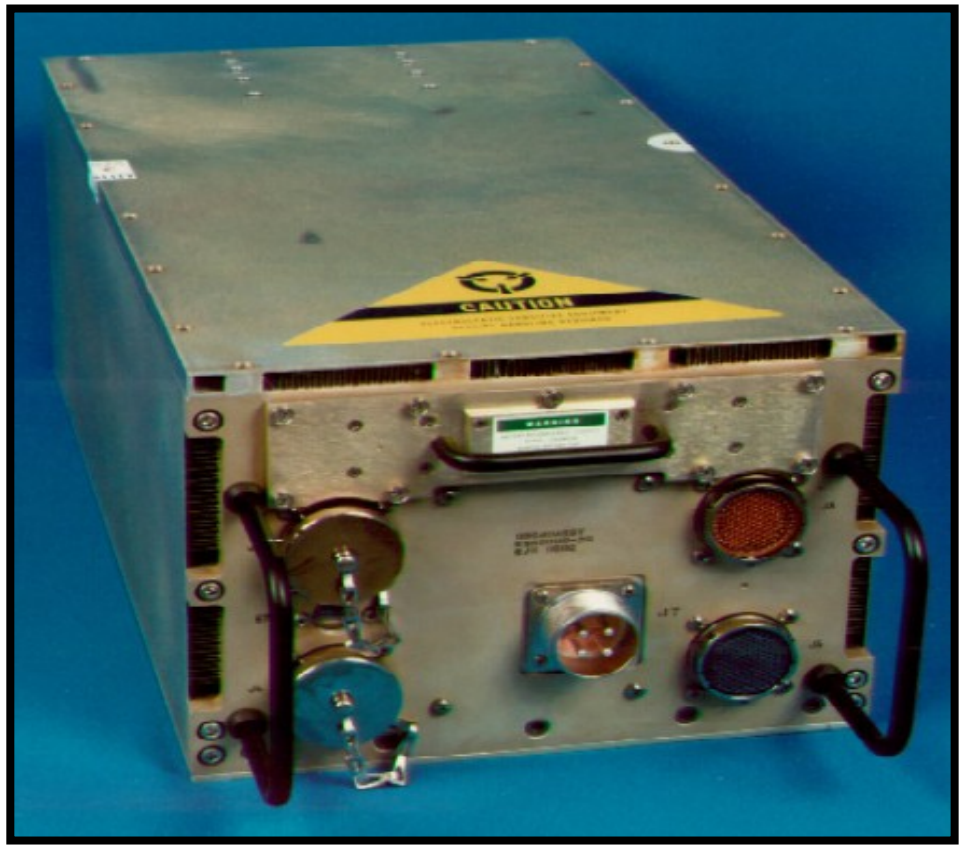
- GPC is the AP 101S constructed by Lockheed-Martin in Owego, NY
  - Can perform 1.3 MIPS
  - Runs the flight software at a clock rate of 25 Hz
    - 25 Hz flight control critical driver for CPU scheduling rates; minimum rates for critical sensor inputs & actuator outputs
  - 1 MB of memory which is completely scrubbed every 1.67 seconds to protect against Cosmic Ray Single Event Upsets (SEUs)
  - Each GPC contains one Input\Output Processor (IOP) that performs all of the I/O across the 24 data buses



Information and Photos courtesy of NASA

GPC (cont.)

- There are a total of 5 GPCs on each orbiter
  - PASS is a real-time, multi-tasking interrupt driven control system with pre-emptive priority scheduling
  - During dynamic flight (ascent and entry) 4 GPCs run PASS Guidance, Navigation, and Control (GNC) software and 1 GPC runs BFS
  - All the GPCs sync up with each other at predefined times such as the completion of an I/O operation
  - The BFS software monitors the state of the orbiter in the case that it is needed due to generic PASS software failure in all PASS GPCs
  - During orbit operations, the orbiter is controlled by 1 GNC GPC and 1 System Management (SM) GPC (except for proximity OPS, i.e. rendezvous)



Information and Photos courtesy of NASA

Error Isolation

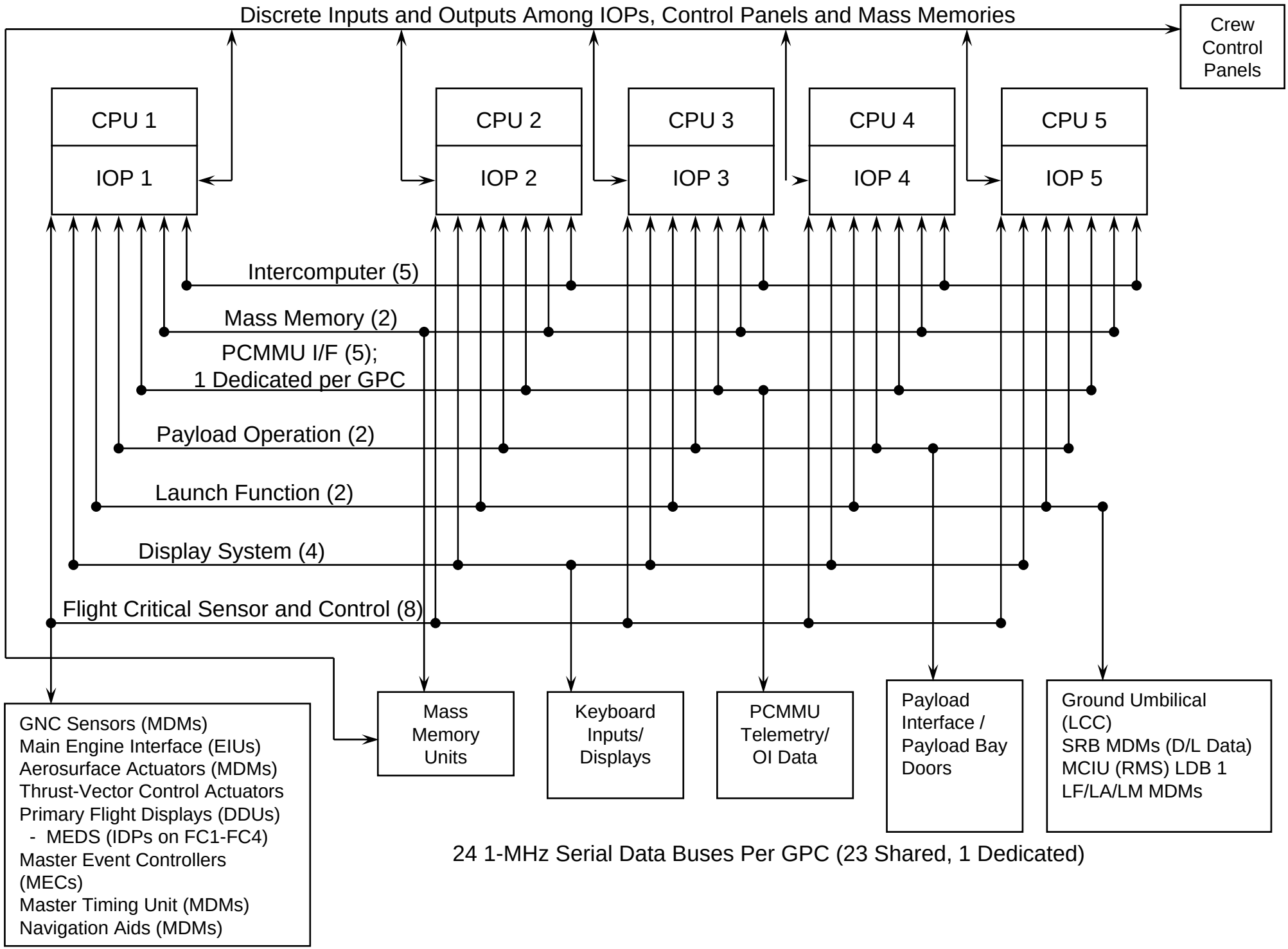
- Redundant set error isolation
  - Isolation is based on information from all GPCs participating in the I/O
  - Uniquely reported error - GPC at fault
  - Multi-GPC reported error - error isolated to bus, Bus Terminal Unit (BTU), and / or element
- If Error is isolated to Bus / BTU / Element
  - Bypassable Transactions
    - Bus Control Element (BCE) Chain Element(s) Bypassed after 2 consecutive errors
  - Non-Bypassable Transactions (e.g. DK Bus poll, LDB poll, etc.)
    - No elimination is performed, i.e. I/O is not suppressed; however I/O Error logging is suppressed after 2 consecutive errors.
- Error is isolated to a GPC (Non-Universal I/O Error)
  - GPC in error will Force Fail to Sync (FTS) after 2 consecutive errors
  - No Automatic Bus Re-Assignments, i.e. each GPC continues to command the buses it commanded prior to the FTS, including the FTS GPC
    - PCMMU Toggle Buffer 1 is assigned to another RS GPC if the remaining RS contains at least two GPCs

IOP

- IOP PROCESSOR ELEMENTS
  - Master Sequence Controller (MSC) Executive Processor:
    - Controls and monitors BCEs, e.g. sets BCE(s) BUSY
    - Interrupts CPU upon I/O completion (Non-MMU transactions)
    - Sets and resets fail vote discretes (CAM)
  - Bus Control Element (BCE): One processor for each of the 24 Data Buses
    - Transmit/Receive data and commands via MIAs
    - BCE Microcode and MIA checks incoming data for errors
    - BCE microcode reads / writes I/O data out of or into memory via DMA
  - MSC / BCE FCOS programs resident in GPC memory (maintained by PASS SSW Development)
  - One or more BCEs can execute the same BCE program concurrently, e.g. FC bus Commander/Listener BCE program
  - MSC and BCEs controlled by FCOS CPU Program Counter Output (PCO) instructions, for example: Load MSC Program Counter, Start MSC, Disable Processors (Put in HALT State), Load Local Store Regs, etc.

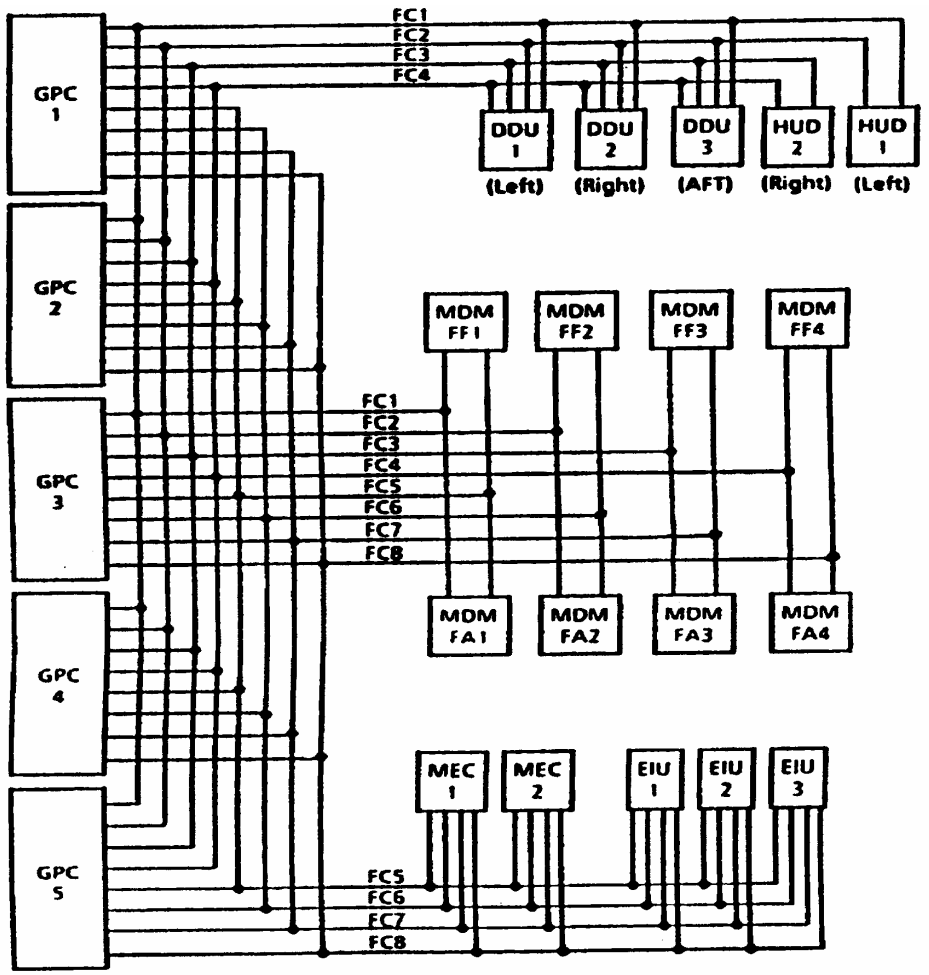
24 Data Buses

- There are a total of 24 buses connected to each GPC
  - 5 Inter-Computer Communication buses allow the passing of status and control information between each of the 5 GPCs
  - 4 Display buses connect the GPCs to 4 Integrated Data Processors that control the 11 MDUs
  - 2 Mass Memory buses connect the GPCs to the 2 Solid State Mass Memory Units
  - 8 Flight Critical (FC) buses connect the GPCs to hardware elements responsible for monitoring the state of the orbiter and controlling its operations
    - The 8 busses are paired together to form 4 Flight Critical strings
  - 2 Launch Data buses provide Kennedy Space Center (KSC) Mission Control with direct communication with the orbiter
  - 1 Pulse Code Modulation Master Unit (PCMMU) bus collects information from different sensors and provide downlist capability for the GPCs
    - 1 Dedicated bus per GPC (all other buses are shared)
  - 2 Payload Data buses allow the SM GPC to perform operations required by different payload devices


Discrete Inputs and Outputs Among IOPs, Control Panels and Mass Memories
Crew Control Panels
CPU 1
IOP 1
CPU 2
IOP 2
CPU 3
IOP 3
CPU 4
IOP 4
CPU 5
IOP 5
Intercomputer (5)
Mass Memory (2)
PCMMU I/F (5);
1 Dedicated per GPC
Payload Operation (2)
Launch Function (2)
Display System (4)
Flight Critical Sensor and Control (8)
GNC Sensors (MDMs)
Main Engine Interface (EIUs)
Aerosurface Actuators (MDMs)
Thrust-Vector Control Actuators
Primary Flight Displays (DDUs)
- MEDS (IDPs on FC1-FC4)
Master Event Controllers (MECs)
Master Timing Unit (MDMs)
Navigation Aids (MDMs)
Mass Memory Units
Keyboard Inputs/ Displays
PCMMU Telemetry/ OI Data
Payload Interface / Payload Bay Doors
Ground Umbilical (LCC)
SRB MDMs (D/L Data)
MCIU (RMS) LDB 1
LF/LA/LM MDMs
24 1-MHz Serial Data Buses Per GPC (23 Shared, 1 Dedicated)

Flight Critical Bus Configuration

- Command of FC buses can be assigned to a GPC or GPCs by “strings”, i.e. pairs of FC buses
  - String 1: FC1 & FC5
  - String 2: FC2 & FC6
  - String 3: FC3 & FC7
  - String 4 : FC4 & FC8
- Command of redundant sensors, actuators, and avionics boxes can be controlled by one GPC or distributed among multiple GPCs for fault tolerance
- Multiplexer/Demultiplexers (MDMs) have dual ports (two Multiplexer Interface Adapters (MIAs)) so they have the capability to receive commands via two buses for better fault tolerance

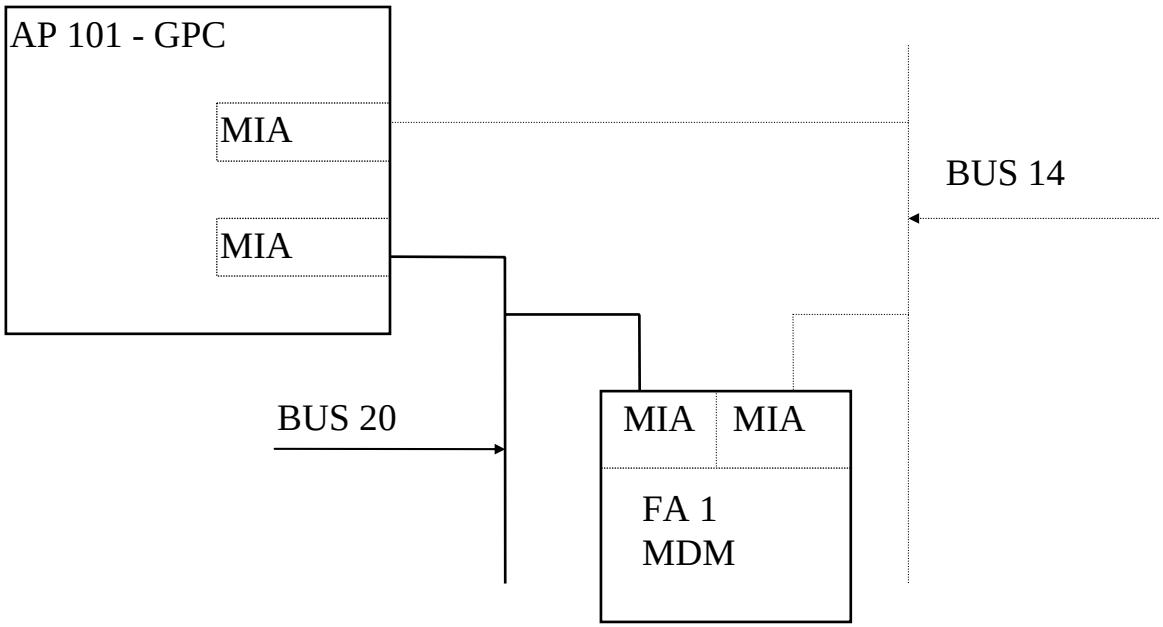


Buses

- Space Shuttle bus system created in the 70's but still applicable today.
- The data bus in use is the precursor to the 1553 bus.
  - 1 Mb per second transfer rate
  - Uses Manchester encoding
- The "cross-strapping" of serial data buses allows each computer in the set to acquire identical inputs
  - The architecture ensures that there is only one commander per bus but the cross-strapping allows each GPC to listen to the transfer
  - This system requires each GPC to be closely synchronized so they remain on the same page
- Port Mode Request on FC String or PL Buses
  - Only the BCE Chains on the moded string / buses are restored
  - All Transaction Error Counters (TECs) for all Device IDs are Reset to Zero

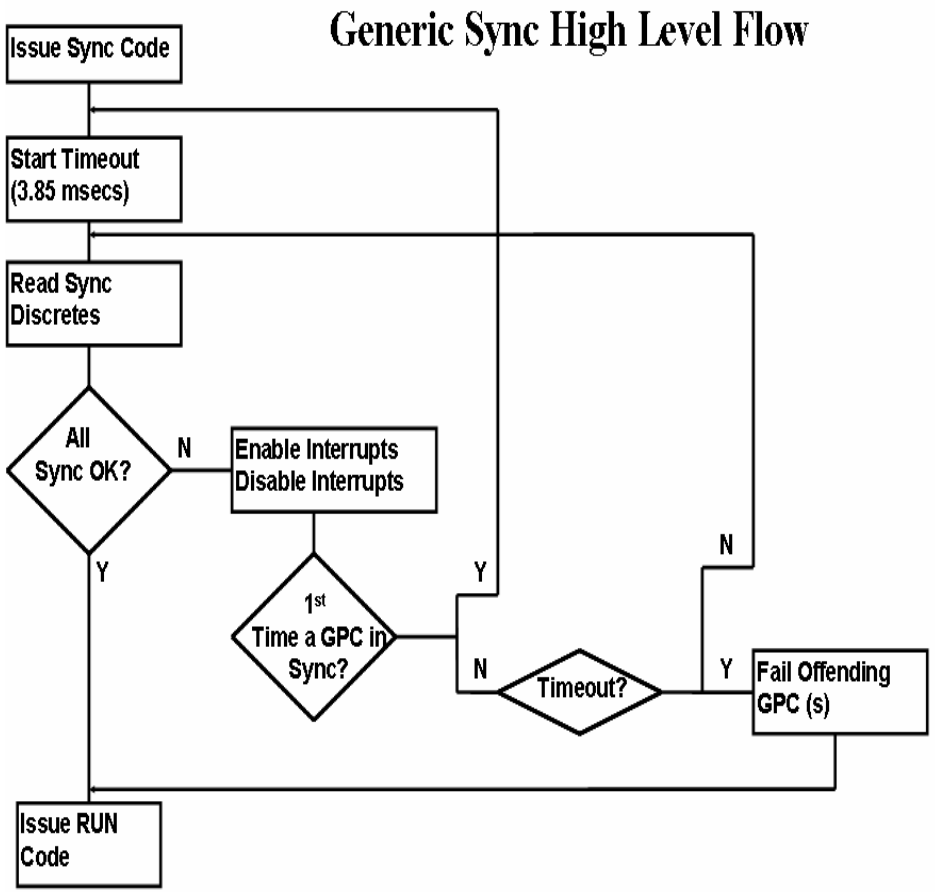
FC/PL Port Mode

- Port mode is a user requested transaction. The request is sent across the ICC buses to ensure that each GPC has the same port mode status.
- For example, each FC MDM is accessible by both buses on a particular string.
  - Primary mode is Bus 20-23 access Flight Forward (FF) MDMs and 14-17 access Flight Aft (FA) MDMs. Secondary mode swaps these assignments.



Synchronization Design

- Identical software executing in different computers are synchronized by arriving at and waiting at sync points. These sync points are inserted for events that can allow process context switches and include support for Timer, I/O completion, and Supervisor Call (SVC) events.
- Each sync point is actually a “Sync Loop” routine with a time out value.
- At the arrival to a sync point, the routine drives a sync code on the three discrete lines and waits in a loop until all expected computers arrive with the same sync code.
- A computer is failed from the set when it fails to arrive with the proper code within a specified time out period.
- The software clock is used to provide a common time in the computers (internal S/W clocks kept in sync by synchronization to a common clock source once every major cycle)



IOP Operations

- MSC and BCE programs control the IOP operations
- MSC processing starts BCE processing and monitors BCE for completion. Once the BCE program completes, the MSC sends an interrupt to the CPU.
- BCE processing is unique for each transaction. It controls the transfer of data to and from the commanded subsystems.
  - BCE modules are collections of BCE programs
    - I/O associated with a particular bus or transaction
    - BCE code varies slightly between commander and listener
    - Each of these programs are reached via multiple entry points related to the I/O, bus number, and commander/listener status
  - BCE programs can be dynamically altered by the PASS System Software to skip transactions that have been bypassed.

Code Example (Commander / Listener)

Commander

- Load the address of the buffer to receive data
- Send out command to device (hard-coded or from the command word table)
- Delay for the listeners to set up
- Read Data (uses hard-coded word counts or word count table)
- Enter wait state or branch/continue to another read

Listener

- Load the address of the buffer to receive data
- Load Interface Unit Address Register
- Receive data (uses hard-coded word counts or word count table)
- Enter wait state or branch/continue to another read