Thierry Bedos
X-38 V201 avionics architect
Matra Marconi Space
31, Avenue des Cosmonautes
31402 Toulouse Cedex 4
France

Brian L. Anderson
X-38 project manager
NASA Lyndon B. Johnson Space Center
2101 NASA Road 1
Houston, Texas 77058-3696
USA

X-38 V201 avionics architecture

1. Introduction

1.1 Context

The X-38 is an experimental NASA project developing a core human capable spacecraft at a fraction of the cost of any previous human rated vehicle. The first operational derivative developed from the X-38 program will be the International Space Station (ISS) Crew Return Vehicle (CRV). Although the current X-38 vehicles are designed as re-entry vehicles only, the option exists to modify the vehicle for uses as an upward vehicle launched from an expendable launch vehicle or from the X-33 operational derivative. The Operational CRV, that will be derived from the X-38 spaceflight vehicle, will provide an emergency return capability from the International Space Station (ISS). The spacecraft can hold a crew of up to seven inside a pressurized cabin. The CRV is passively delivered to ISS, stays up to three year on-orbit attached to ISS in a passive mode with periodic functional checkout, before separation from ISS, de-orbit, entry and landing. The X-38 Vehicle 201 (V201) is being developed at NASA/JSC to demonstrate key technologies associated with the development of the CRV design. The X-38 flight test will validate the low cost development concept by demonstrating the entire station departure, re-entry, guidance and landing portions of the CRV mission. All new technologies and subsystems proposed for CRV will be validated during either the on orbit checkout or flight phases of the X-38 space flight test The X-38 subsystems are required to be similar to those subsystems required for the CRV to the greatest extent possible. In many cases, the subsystems are identical to those that will be utilized on the Operational CRV.

1.2 Mission

The mission of the X-38 V201, unpiloted space-flight test vehicle, is composed of several phases. The vehicle will be launched from the Space Shuttle Orbiter and placed in a circular or near-circular orbit. The X-38 vehicle is launched unpowered in the Shuttle Bay. Once on orbit, the vehicle is checked-out during a maximum duration of three days in the Shuttle Bay. During the three day period in the shuttle bay, the program will exercise procedures and test subsystem equipment to validate concepts for the monthly checkout that will be required of the operational CRV once it is attached to the ISS. The vehicle is deployed with Shuttle RMS and separated from the Shuttle. The De-orbit Propulsion Stage (DPS) is activated when the Shuttle is at a safe distance. The de-orbit burn is performed after a few hours of on orbit loiter, and ends with the DPS jettison. During the loiter phase, the vehicle will plan its own de-orbit burn, monitor its systems health, and make any isolation and recovery actions required to maintain control and system maintenance prior to and during reentry. After a de-orbit coast down to 400,000 feet altitude, the entry starts under control of the on board Attitude Control System (ACS) first, then of aerosurfaces, 2 body flaps and 2 rudders, when dynamic pressure becomes sufficient. The drogue parachute is deployed at 23,000 feet altitude and the parafoil deployed for landing. The maximum operational life of the X-38 is 9 hours. Planned time for the V201 mission is 5 to 7 hours from Shuttle deployment to landing.

1.3 Requirements

1.3.1 General objectives

The V201 avionics architecture is designed to be at least single fault tolerant, to maximize commonality with CRV, and in compliance with the Shuttle payload requirements. One of the main architectural requirement that has been placed on the project is to take advantage of Commercial Off The Shelf (COTS) equipment and already developed technology for as much as 80 percent of the spacecraft's design. The X-38 flight computer is COTS equipment, as well as the flight software operating system. Most of the avionics equipment units are also COTS. Development of new units is limited to a strict minimum. Other technological choices include: fiber optics data transmission, Electro-Mechanical Actuators (EMA) activating the aerosurfaces, Space Integrated Global positioning system /Inertial navigation system (SIGI) and laser pyrotechnics.

1.3.2 Failure tolerance requirements

The failure tolerance is based on the CRV approach, aiming to guarantee 1 failure tolerance at separation from the Space Station. While docked to the Space Station, periodic checkout will allow detection of possible failures. Inside the cabin, it is possible to replace a failed unit. Therefore, the architecture is required to be 1 failure tolerant within the cabin although dual fault tolerance of critical systems is being pursued. Outside of the cabin, it is not feasible to perform ExtraVehicular Activities (EVA's) to replace a failed unit, therefore the architecture is required to be 2 failure tolerant in all critical external systems.

1.3.3 Tolerance to the loss of 2 FCC's

The vehicle must be able to safely operate and land in the event that 2 FCC's are lost (a loss being defined as inactive or powered-down FCC). The vehicle is required to maintain control with <u>any</u> 2 FCC's although the control may be degraded after the second loss. The architecture therefore must be organized so that the loss of associated major sub-systems will not prevent the vehicle from performing the mission: SIGI's, pyros, propulsion and EMA's. Total or partial loss of other sub-systems is considered not to be critical due to the short mission duration. For CRV, crew intervention will be required for safing actions such as wearing O2 masks or manual actuation of valves. It must be noted that the tolerance to the loss of 2 FCC's does not allow the vehicle to withstand any failure of 2 FCC's. While the vehicle can withstand most of double failures, some combinations of simultaneous fault commands from 2 FCC's can be catastrophic. As an example, 2 simultaneous fault commands generated by 2 different FCC's can activate ARM and FIRE for the same pyro function of a Laser Firing Unit (LFU), leading to inadvertent initiation of this pyro event. These failures, although theoretically possible, are considered highly improbable and unrealistic. The additional equipment and architectural complexity required to protect against all potential "smart" failures, could in many cases, actually decrease the reliability of the vehicle. The project has chosen not to protect against these unrealistic failure scenarios.

2. V201 avionics architecture description

2.1 Overall architecture

The V201 avionics architecture is depicted in Figure 1.

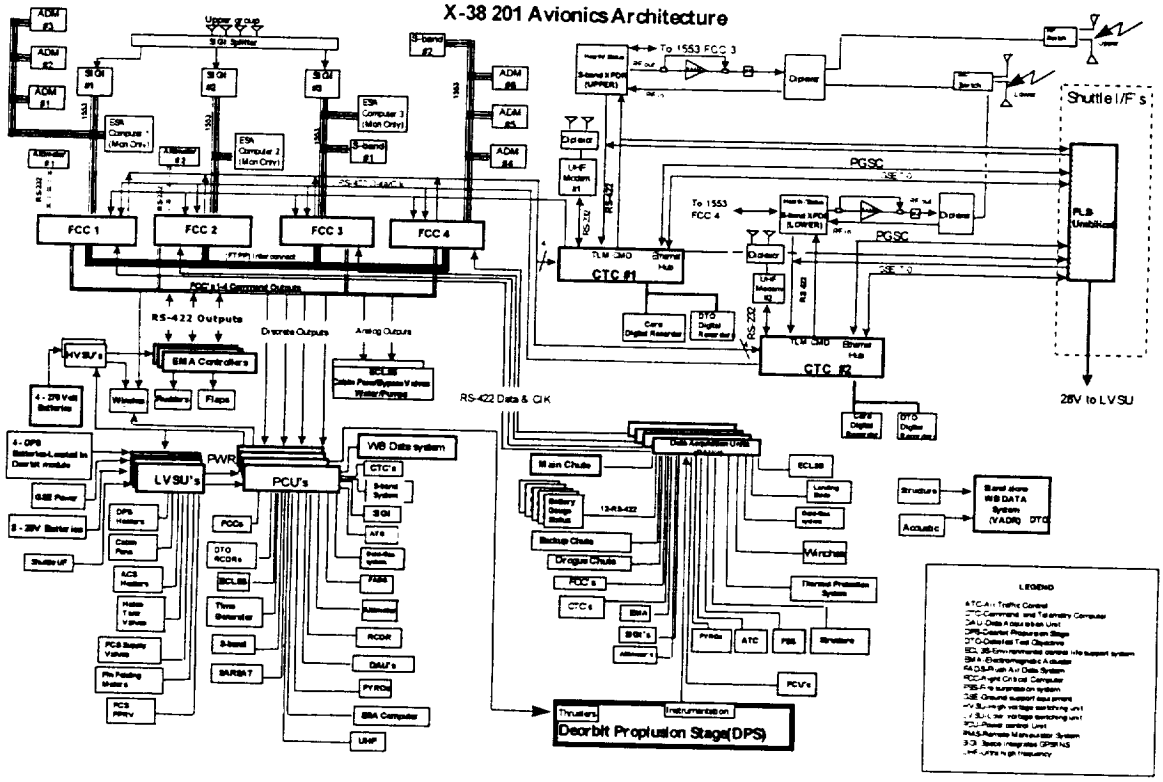

Figure 1 : X-38 V201 avionics architecture

The architecture is organized around four major poles :

- Fault Tolerant Parallel Processor (FTPP) in charge of overall vehicle control.
- Electrical Power Distribution and Control box (EPDC) composed of Low Voltage Switching Units (LVSU's), Power Control Units (PCU's) and High Voltage Switching Units (HVSU's) in charge of power generation and distribution ;
- Data Acquisition Units (DAU's) in charge of data acquisition ;
- Control and Telemetry Computers (CTC) in charge of Communications, Shuttle data interfaces (S-band, UHF and Ethernet), and recorders.

2.2 FTPP

The FTPP is composed of four identical Flight Critical Computers (FCC's), providing Byzantine failure resilience. The FCC's are assembled from COTS chassis and boards, and use commercial VxWorks operating system. The processor board is Radstone PowerPC 604e board. The only board developed for this application is the Network Element board (NE). The FCC's exchange and vote data using a 100 Mbps fiber optics data network. Each FCC has a specific power supply and controls a part of the vehicle architecture, organized as a Fault Containment Region (FCR). Redundant sub-systems are connected to FCC's I/O's such as to provide the required failure tolerance. The FTPP Byzantine failure tolerance is based on the services provided by Fault Tolerant Software Services (FTSS) and the NE boards. The FTPP is designed to tolerate two permanent, sequential processor failures. It is also designed to discriminate

between transient faults, such as those caused by Single Event Upsets, and permanent faults and to recover hardware resources affected by transient faults. The NE ensemble is synchronized with a distributed fault tolerant clock. NE's maintain time synchronization of all FCC's and manage data exchanges allowing them to make input data congruent and to vote computed outputs. After a transient FCC failure, the FTSS allows the FCC to re-synchronize by aligning its memory. Due to the required duration, this capability will not been used during critical mission phases. In case of transient or permanent failure, power delivered to each FCC can be recycled or switched-off, as voted by the other FCC's.
SIGI, Flush Air Data System (FADS) and S-band transponders are connected to the computers using MIL-STD-1553B buses. Serial lines connect the computers to the Altimeters, EMA controllers, DAU's and to the CTC's.
The selection of the type of data link is based on technological choices, expected performances and previous projects heritage:

- RS422 serial lines have been used as much as possible providing a robust link and minimizing the interconnection. They are used to control the EMA's, to receive the acquisition frames generated by each DAU and to communicate with the CTC's. Each FCC sends 4 telemetry streams, one to each CTC, and receives 2 uplink command links, one generated by each CTC.
- the FTPP requires an interconnection with high data throughput : the Network Elements (NE) exchange data at 100 Mbps through fiber optics network ;
- the FCC sends TTL commands to control PCU power distribution switches, such as to keep the PCU as simple as possible.
- analog commands are used for some sub-system functions : Environment Control and Life Support (ECLS) heat exchanger by-pass valve position, water pump speed and cabin fan speed, as well as parafoil winch rate.
- other serial lines are used based on COTS constraints. Radar altimeters are connected to FCC's through RS232 links. FCC's MIL-STD-1553B buses are used to control SIGI's, FADS, and S-band transponders. Three ESA computers monitor the MIL-STD-1553B bus activity in order to acquire SIGI data and validate diversified GNC algorithms. No command is generated by the ESA computers, which have no command output.

Inputs/output capability has been implemented in the FCC in order to simplify the overall architecture. Each FCC uses a NE board for FTPP internal exchanges on the fiber optics network. Each FCC has two processor boards that provide significant processing power margin compatible with the FTPP concept. One processor board is dedicated to flight critical processing, while the other manages data acquisition and commands. Direct serial line connection to EMA's has been selected in order to minimize the control loop latency. An IRIG decommutation board allows acquisition of time information from the IRIG time generator and receipt of the DAUacquired data.
Most of the sub-systems are controlled by switching LVSU and PCU power feeds under direct control of the FCC.

2.3 EPDC

The power distribution architecture is provided in Figure 2.

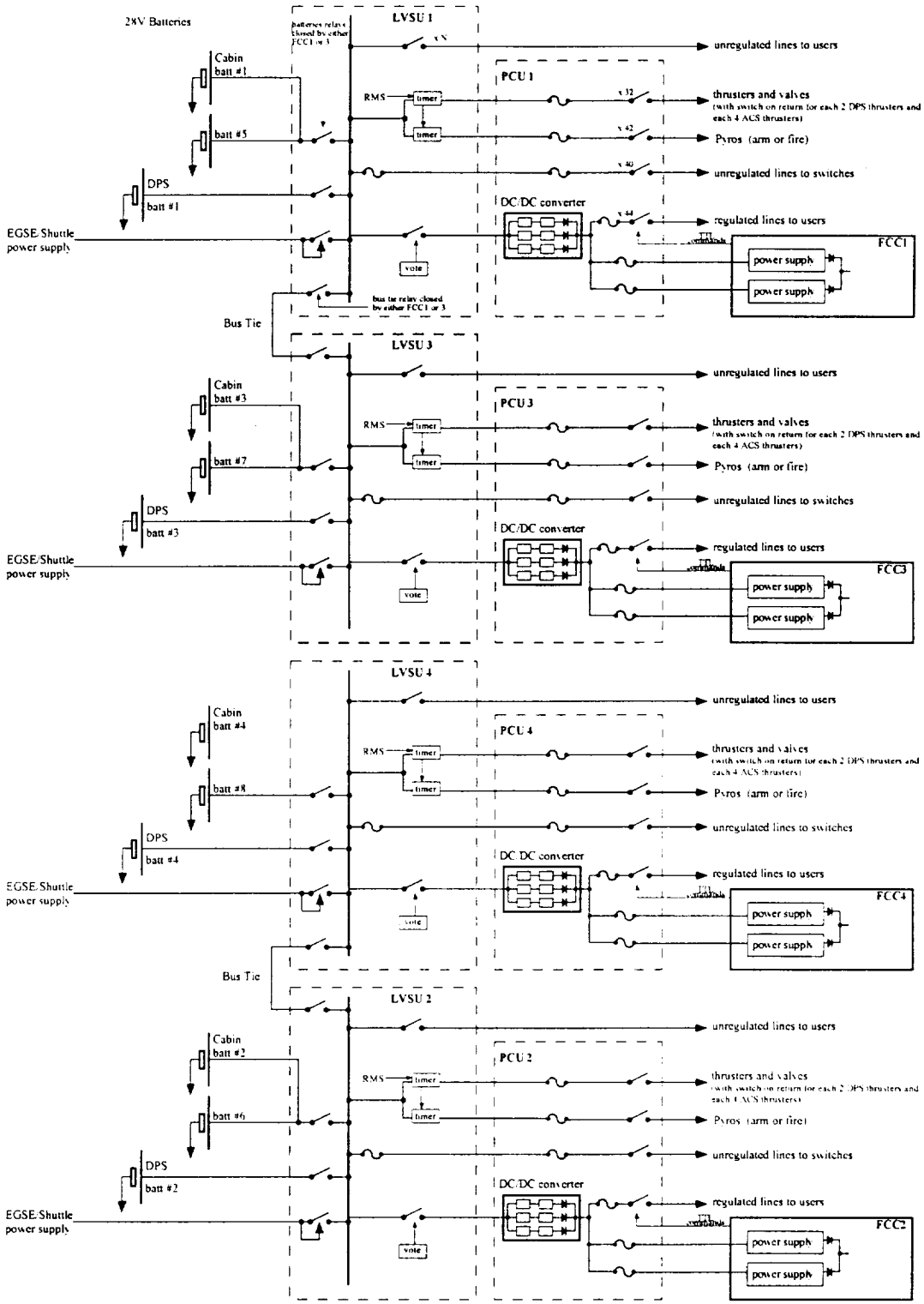

Figure 2 : power distribution architecture

The power is provided from external sources for ground or attached phase (EGSE or Shuttle) or from 28V batteries (LiMn02 DPS batteries after separation from Shuttle, NIMH cabin batteries after DPS jettison). The 270V system has its own NiCd high voltage battery set. Four power channels provide independent power to each of the four FCC's and to the associated FCR. External power sources are connected to the LVSU bus by electro-mechanical relays. The PCU solid-state switches are controlled by FCC TTL commands and provide direct command and power distribution to users. Regulated power is provided to a part of the loads, basically all electronic units, while unregulated power is used by thrusters, valves, pyros and switches. Large consuming unregulated loads, such as heaters, fans, motors and motorized valves, are connected directly to LVSU relays. In the PCU, hardware timers are implemented to provide inhibits additional to FCC software control as required while the 201 vehicle is in the Shuttle vicinity. RMS contacts initiate timers which connect propulsion and pyros after a time delay, allowing activation of the ACS about 5 minutes after separation and DPS about 45 minutes after separation, thus meeting the minimum separation distance requirements.
Some cross-strapping of commands are implemented from PCU's to LVSU's. When one FCC is lost, the neighbor FCC can connect the batteries of the lost FCC to its own LVSU bus through the bus tie. Another cross-strapping allows control of the power feed of each FCC, and power down of a failed FCR, when a majority of 2 FCC's decide so. The PCU switches control also the HVSU switches in charge of connecting the 270V batteries and distributing power to EMA's and winches.

2.4 Instrumentation system

There are 4 DAU's. Each DAU acquires sub-system sensor data and provides a PCM serial stream to one FCC only as part of its FCR. DAU's inputs are of various types: analog single ended, analog differential, bridge completion, RTD, thermocouple and digital. Mini-DAU's are embedded in PCU's and send their PCM output to the DAU of the same FCR.
A DTO wide band data acquisition system, the Vehicle Analysis Data Recording system (VADR), is in charge of structural and acoustic data acquisitions. It is made of 1 Data Handling System, 10 front end electronic boxes, 2 Signal Processing Units, 1 Pyrometer Electronic Box and 1 mini DAU. During the launch phase, the VADR is directly powered from Shuttle interface for recording of launch data.

2.5 CTC system

The CTC's system is fully redundant. Each CTC controls its own set of UHF, S-band, recorders and Shuttle interfaces, without cross-strapping. Data links with FCC's and power interfaces of each CTC are cross-strapped. Each CTC receives the telemetry link generated by each of the 4 FCC's and sends its uplink command link to each FCC. Each CTC receives 2 power feeds from 2 different PCU's. The CTC is based on the same chassis and power supplies used for the FCC. Most of the boards are the same as the FCC boards. Specific boards are Ground Communication Encoder and Decoder, and Ethernet interface.

2.6 Sub-systems

Sub-systems redundancy and failure tolerance depends on their criticality.

2.6.1 Two failure tolerance implementation

The redundancy and cross-strapping allows control of the major sub-systems with 2 FCC's only.

2.6.1.1 Pyros

Each pyro event is controlled by redundant initiators. Pyro lasers have been selected due to their excellent EMI immunity. A total of 20 pyro events are necessary for deorbit module activation, deorbit module separation, primary and back-up chute sequence and landing gear deployment. Activation of 6 flash lamps illuminate laser rods which send the laser energy to the initiators. In each LFU, two commands are necessary for each pyro event: 1 arm command, controlling an optical shutter and a fire relay, and 1 fire command that applies the power to the flash bulbs. The tolerance to the loss of 2 FCC's is implemented by having redundant interfaces for all arm and fire commands of each LFU. Each functional command can be

controlled by 2 FCC's. The interconnection guarantees activation of at least one initiator for each pyro event with any couple of 2 FCC's. The interconnection is shown on Figure 3.

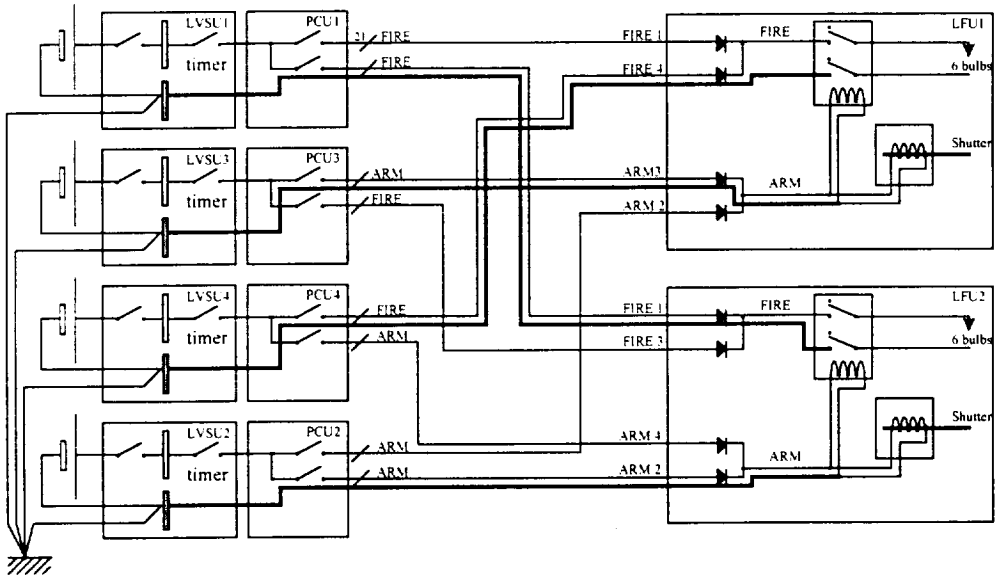

Figure 3 : Pyros control interconnection

2.6.1.2 EMA's

The EMA's are configured to be two fault tolerant with each actuator based on three channels composed of one controller and one motor. The typical control configuration of one aerodynamic surface is shown on Figure 4. One channel is sufficient to ensure the performance required by the aerosurface. Each channel is mechanically connected to the control surface mechanism by a clutch. A brake allows the EMA to lock the aerosurface during the launch phase and at the end of the active phase. The clutch and brake are automatically controlled by application of the power to any of the 3 channels. Each channel is controlled by a different FCC, with interconnection allowing control to each aerosurface after the loss of 2 FCC's. The architecture provides fault masking of the first failure: the 2 healthy channels maintain the performance for any behavior of the failed channel. However, motors can not withstand the high power dissipation resulting from the conflicting torques and the failed channel must be isolated in about one second. The FCC controlling the failed channel will try to isolate it. If it can't, the FCC itself will have to be isolated by the other FCC's, using the voter on the power supply.
On the second failure affecting the same actuator, the fault is not masked. Conventional detection and isolation process shall be performed.

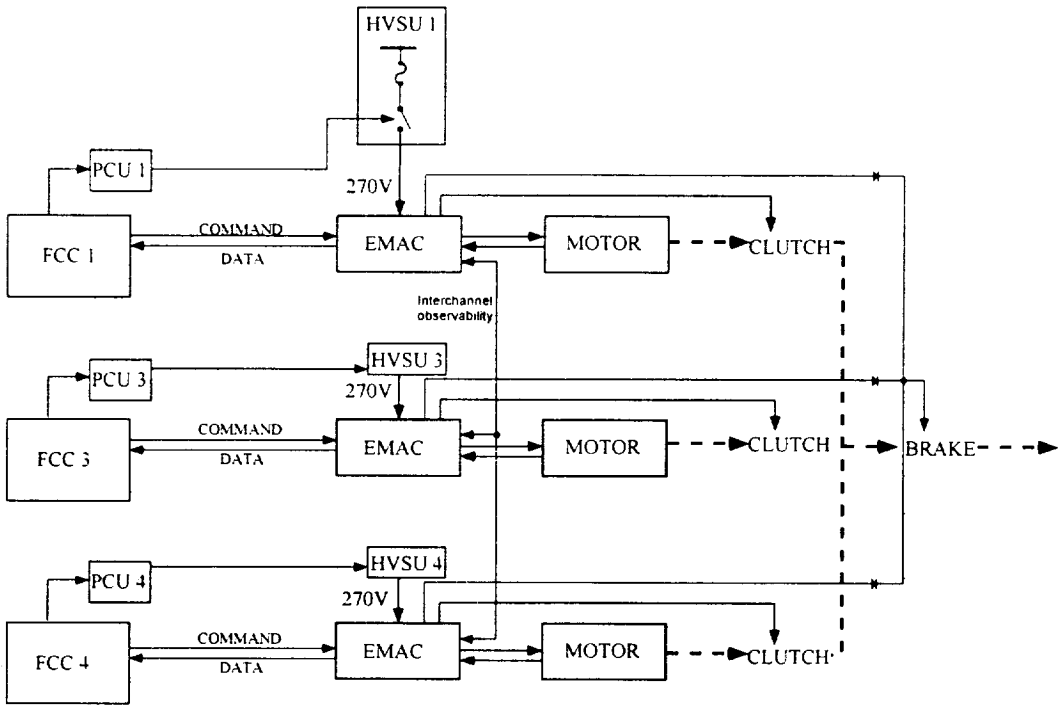

Figure 4 : Control of one aero-surface

2.6.1.3 SIGI's and RF FE

The SIGI is a self contained, all attitude inertial navigation system with a tightly coupled GPS receiver within a single chassis providing vehicle position, velocity, acceleration, altitude, attitude rate, and time. There are three SIGI's. Each SIGI is connected to one FCC and receive its power from the same FCR. Four antennas and pre-amplifiers are used for GPS attitude determination that requires a minimum of 3 antennas. GPS signal is distributed from each antenna to all SIGI's using power dividers. In order to face the loss of 2 FCC's during the initial attitude determination, each pre-amplifier must have redundant power feeds from 2 FCR's.

2.6.1.4 DPS and ACS propulsion

The Hydrazine DPS has been designed to be as simple as possible. A set of 3 tanks is connected with pyro-valves to a set of 8 main deorbit thrusters and a set of 8 reaction control thrusters. There is no isolation valve. Isolation of a thruster is based on double seat control valve (for mechanical failure) and multiple switching on the electrical command. In addition to the FIRE activation switch implemented for each thruster, an ARM switch is implemented on the return line. There is on return switch for each reaction control thruster, and one return switch for each couple of deorbit thrusters. Each pair of thrusters is allocated to a different FCR, to maintain at least 6 operating thrusters after the loss of one FCR. In order to withstand the loss of 2 FCR's, cross-strapping of commands has been added, allowing the system to maintain control of 6 DPS thrusters. Any pair of thrusters can be controlled by two FCC's. The ARM power return switching is used to prevent return current loop. The cross-strapping principle is shown on Figure 5.

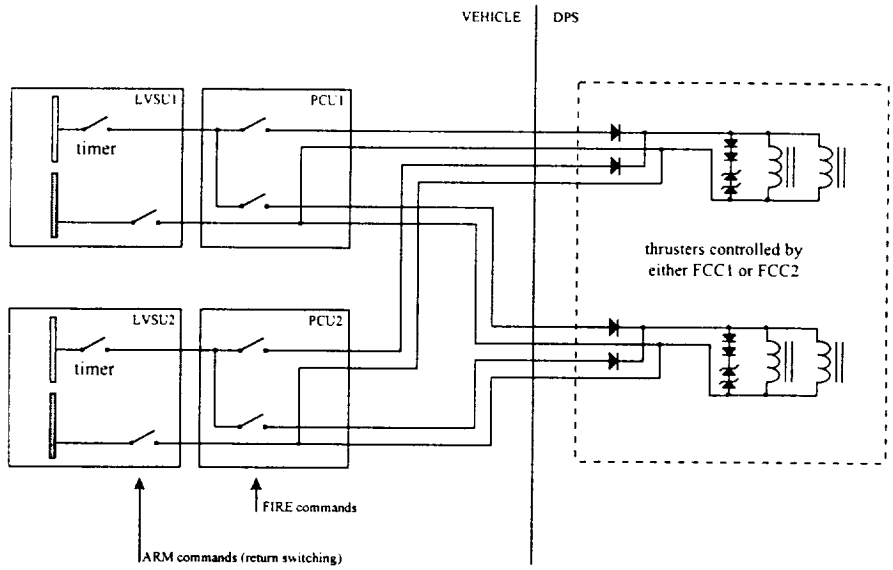

Figure 5 : cross-strapping of DPS thruster commands

The cold gas ACS is composed of rear and aft manifolds. The forward manifold is a DTO to validate attitude control at separation from the Space Station. Therefore, it is a single chain with no redundancy. The aft manifolds are organized on complete redundant chains. Each chain has isolation valves controlled by one FCC, while a different FCC controls the thrusters. Cross-strapping of commands to isolation valves and thrusters has been added, with interconnection to guarantee full control of one aft manifold after the loss of 2 FCC's. The same FIRE and ARM switching as for DPS control has been implemented based on groups of 4 commands with a common return switching.

2.6.2 One failure tolerant avionics subsystems

Most individual avionics subsystems are one failure tolerant. Each subsystem redundancy is part of a single FCR.

2.6.2.1 recorders

Core and DTO recorders are solid state recorders, connected to one CTC through SCSI interface. The core recorders provide nominal flight recording capability while DTO recorder provide additional capability for the V201 demonstrator.

2.6.2.2 S.band

The S-band system provides RF communications with ground controllers via Tracking and Data Relay Satellite System (TDRSS), Ground Spaceflight Tracking and Data Network (GSTDN) sites and Shuttle (via Payload Interrogator & Ku-band bent-pipe D/L only). The X-38 S-band System can transmit telemetry to the Shuttle S-band Payload Interrogator which is then sent via Shuttle Ku-band bent-pipe (Mode 2 FM, Channel 3) to TDRSS.
Planned operation is to continuously operate with TDRSS through landing. One transponder will be configured to transmit at high data rate during proximity operations with Shuttle and when in view of GSTDN sites. At other times both transponders will be in the TDRSS mode. The vehicle computer software will determine which hemisphere to switch antenna (upper/lower).

2.6.2.3 UHF

The UHF system provides Shuttle astronaut control and monitoring during deployment phase and ground based parafoil control during the landing phase.

The X-38 PGSC's inside the shuttle will be connected to the 2 UHF Radios to provide a means to receive telemetry and send commands from/to the X-38 V201 vehicle. The UHF link will be used by the crew during proximity operations (post-umbilical separation) to monitor high level vehicle status. It also provides the crew the capability to send a "kill" command to the X-38 V201 if necessary. This command will suspend all vehicle functions and place the vehicle in a safe, passive state. This Shuttle Crew command path is supported by two PGSCs and two UHF Radios each with its own window mounted antenna.

2.6.2.4 Altimeter

The radar altimeter provides accurate altitude measurements for final vehicle navigation under the parafoil. During the mission, the altimeter will be switched on in the final minutes of flight. Its primary purpose is to provide final altitude in order to determine when to execute the parafoil flare maneuver.

2.6.2.5 FADS

The FADS consists of 9 pressure ports oriented in a crucifix configuration at the nose of this vehicle. Five ports in the XZ plane are used to compute angle-of-attack, and five ports are used in the XY plane to compute side-slip-angle. All of the pressure ports are used to compute mach number, ambient pressure, altitude, true airspeed, and dynamic pressure. The design of the FAD system is single fault tolerant. Each port is connected to 2 acquisition modules. FADS is organized on two redundant chains. Each chain is composed of 3 modules with each module connected to 3 pressure ports. FADS operation starts at Mach 2.5 and continues to operate all the way down to landing.

2.6.2.6 time generator

Two IRIG B time generators provide time information to the FCC's.

2.6.3 Avionics subsystems with no failure tolerance

2.6.3.1 ATC

The ATC transponder provides the air traffic control a means to track vehicle. The ATC will be started at 55,000 feet altitude.

2.6.3.2 SARSAT

The SARSAT ELT provides beacon signal to satellite and homing signal to ground forces in a off-nominal landing situation. Power is provided by a self-contained $LiMnO_2$ battery with 48 hours of life. SARSAT operations is initiated by an impact sensor.

2.7 Other sub-systems with major interface with avionics

2.7.1 ECLS

ECLS is mainly composed of one redundant heat transport and rejection function, based on 2 water loops with sublimators and 1 air loop with redundant fans, and one redundant Pressure Control System (PCS) providing O2 and N2 for atmosphere control and tank pressurization. Each heat transport and rejection loop is controlled by one FCC. The four FCC's are involved in PCS control. For one chain, one FCC controls the supply valves while another FCC controls the flow control valves. The two other FCC's control the redundant chain. One of the FCC's controlling the flow control valves controls an interconnecting valve between both chains. With this interconnection, no single failure can prevent the system from using at least one redundant path nor from isolating a failed open valve.

2.7.2 Fin folding mechanism

Each vehicle fin is folded in the Shuttle bay in the launch configuration. It is deployed by two motors when the Shuttle bay is opened. The avionics provide power to the fin folding motors and monitors the micro-switches status. Each motor is powered from one FCR, since one motor is sufficient to deploy the fin. The motor can not withstand the high current when it is stopped on the mechanical stop. The PCU provides current limitation by one solid state switch, and LVSU provides 2 relays, one for direction selection and one for activation. This last relay can be used by the software as a final safing device with regard to possible failures of the current limiter.

3. Conclusion

The here-above description shows how it is possible to build a dedicated architecture based on maximum re-use of existing equipment, and minimizing new development to a strict minimum. Due to the project development status, the described architecture reflects the current baseline, but can not be considered to be the final V201 avionics architecture.