Integrated Modular Avionics (IMA)
• Developed by Ron Szkody in 1996
• IMA is a Honeywell provided hardware and software abstraction layer that allows the Orion program to operate a robust, modular, and easily scaled design
• Decentralizes the logically grouped computational units (ex. Guidance and Navigation) through the use of a “Virtual Backplane”
• Allows the Orion team to operate at the Application layer and communicate through the Virtual Backplane via a standardized API
• Applications or “Partitions” (ex. GNC) are time and space partitioned
• Memory resources (size and location) are pre-allocated with write access only allowed by the partition
• Computational resources are pre-determined as well with a set time and duration allotted for each partition
• Handled by the OS (Greenhills Integrity OS) and configured using XML files
• The system is driven by one interrupt (frame sync)
• Applications or “Partitions” (ex. GNC) are time and space partitioned
• Memory resources (size and location) are pre-allocated with write access only allowed by the partition
• Computational resources are pre-determined as well with a set time and duration allotted for each partition
• Handled by the OS (Greenhills Integrity OS) and configured using XML files
• The system is driven by one interrupt (frame sync)

Backup Flight Software utilizes a unique architecture to prevent against common cause failures
Time-Trigger Ethernet for the Onboard Data Network (ODN)
• ODN is a 1 Gbps, Time-triggered, tiered Ethernet operating on 3 redundant planes
• Eliminates Automatic Dynamic Reconfiguration

<table>
<thead>
<tr>
<th>Tier 1</th>
<th>Time-triggered messages: transmitted over the network at a predefined time with guaranteed delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 2</td>
<td>Rate-constrained messages: design for less determinism, but guaranteed bandwidth</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Best effort messages: Used as part of the remaining bandwidth with no guarantees of transmission (ex. Video)</td>
</tr>
</tbody>
</table>
Notes:
 Only major components shown
 ODN
  - Plane 1 Blue
  - Plane 2 Red
  - Plane 3 Green
- 18 Network Switch Cards (NSC)
- 46 End System Network Interface Controllers (NIC)
 Serial/other – not shown
 LAS not shown

CMU1
CMU2
SM
ESA SM
CMA
SM
Ground / Lab

Command Telemetry Unit
ECUT | ECAS | ETLM
Other EGSE End Items
Ground Power Unit

Antenna

PDU S1
NSC3
NSC2
NSC1
PDU S1b
NIC
PDU S2
NSC3
NSC2
NSC1
PDU S2a
NIC
PDU S2b
IOMs
PDU S1a
IOMs

ST1

PDU C1
NSC3
NSC2
NSC1
PDU C1a
IOMs
PDU C1b
IOMs

PDU C2
NSC1
PDU C2b
NIC
PDU C2b
IOMs

PDU C3
NSC1
PDU C3a
IOMs
PDU C3b
IOMs

PDU C4
NSC1
PDU C4a
IOMs
PDU C4b
IOMs

PDU C6
NSC1
PDU C6a
IOMs
PDU C6b
IOMs

SM

TCU1
SAD1
SAD2
CMU1
CMU2
TCU2
PDE1
PCDU1
PDU 1
NIC

VMC1
FCM1
DCM1
CCM1
OSM1

VPU1
DDR

OIMU1
IOMs
OIMU2
IOMs

OSM2
NIC
VMC2
FCM2
DCM2
CCM2

OSM
VPU2
DDR

OIMU3
IOMs
OIMU4
IOMs

Antenna

S1
S2

Ground
Lab

Command
Telemetry
Unit

Other
EGSE
End
Items

Ground
Power
Unit

CMU

DAU
SM

CMU

DAU
SM

CM Unpres

CM Press

Transponder 1
Baseband Processor 1

Transponder 2
Baseband Processor 2
Notes:
- Only major components shown
- ODN
  - Plane 1: Blue
  - Plane 2: Red
  - Plane 3: Green
- Network Switch Cards (NSC)
- End System Network Interface Controllers (NIC)
Notes:
- Only major components shown.
- ODN
- Plane 1: Blue
- Plane 2: Red
- Plane 3: Green
- 18 Network Switch Cards (NSC)
- 46 End System Network Interface Controllers (NIC)
- Serial/other – not shown
- LAS not shown

- Command Telemetry Unit
- Ground/Lab
- Command Power Unit
- Ground/ Lab
- Other EGSE End Items
- ETSO

- VMC
- FCM
- OSM
- CCM
- DDR
- OIMU
- VPU
- NIC
- CM Unpress
- CM Press
- CMU
• **Common cause failures**
  - Bug in flight software

• **Radiation hits**
  - Bit flip

• **Dead bus**
  - Power failure

• **Flight and ground crew**
• Common cause failures
  o Bug in flight software

• Radiation hits
  o Bit flip

• Dead bus
  o Power failure

• Flight and ground crew
- **Common cause failures**
  - Bug in flight software
- **Radiation hits**
  - Bit flip
- **Dead bus**
  - Power failure
- **Flight and ground crew**
• Common cause failures
  o Bug in flight software

• Radiation hits
  o Bit flip

• Dead bus
  o Power failure

• Flight and ground crew
• **Common cause failures**
  
  o Bug in flight software

• **Radiation hits**
  
  o Bit flip

• **Dead bus**
  
  o Power failure

• **Flight and ground crew**
How do we recover?
<table>
<thead>
<tr>
<th>Question</th>
<th>Question</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where are we in flight?</td>
<td>What flight computer is in control?</td>
<td>Is there only one flight computer down?</td>
</tr>
<tr>
<td>How do we transfer all the state data across a deterministic network?</td>
<td>What should we do with commands during a reboot?</td>
<td>Have we started a maneuver?</td>
</tr>
<tr>
<td>How do you know when the flight computer outputs are valid?</td>
<td>When should we switch from the backup to the primary flight computers?</td>
<td>If the crew is unconscious, when would we auto enable the outputs?</td>
</tr>
</tbody>
</table>
Partitions owners chose a specific set of data to transfer across the ODN to allow the redundant partition to converge their datasets.

A partition controller tells the other partitions what type of reset occurred based on input data available.

Partitions initialize and converge independently following direction from the partition controller.
• A flight computer should come back into the working set around 20 seconds

• Probability that all flight computers are reset in the same 20 second window is greater than one in 1,870,000 missions
  o The Shuttle never had to enable the Backup Flight Software for any of their nominal missions

• In most cases, the ground or crew must command the reset flight computer back into the working set

• Only failures in critical partitions can reset the entire flight computer