Fault Tolerant ADIRU

- The Boeing 777 has two inertia units,
  - the ADIRU (Air Data Inertial Reference Unit) and
  - the SAARU (Secondary Attitude and Arial Data Reference Unit)
- We will look at the ADIRU, based on the discussion in the paper
  - A Fault-Tolerant Air Data/Inertial Reference Unit
    » Michael L. Sheffels
    » IEEE AES Systems Magazine, March 1993
Fault Tolerant ADIRU

- Air Data/Inertial Reference Unit
  - ADIRU production unit
Fault Tolerant ADIRU

- **Main features**
  - inertial and air data reference for ARINC 651 Integrated Modular Avionics distributed architecture
  - low life cycle cost
  - deferred maintenance
  - high reliability
  - high integrity fault detection
  - fault isolation
  - redundancy management
  - quad channel redundancy
  - robust partitioning
  - simple serial internal interfaces
  - simple voting
  - 3 ARINC 629 bus interfaces
Fault Tolerant ADIRU

Architecture
- 5 basic functions required for operation, referred to as *Fault Containment Areas* (FCA)
  » processor
  » gyro
  » accelerometer
  » ARINC 629 interface
  » power supply
- Individual resources making up a FCA are referred to as *Fault Containment Models* (FCM)
  » each FCA can tolerate the loss of 2 FCMs
  » third failure will cause loss of the ADIRU
  » ARINC 629 interfaces differ
Fault Tolerant ADIRU

FCA = Fault Containment Area
FCM = Fault Containment Module
**Fault Tolerant ADIRU**

- Requirements

<table>
<thead>
<tr>
<th>FCA</th>
<th>Function</th>
<th>Dispatch</th>
<th>Deferred Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Gyro</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Accelerometer</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Power Supply</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>ARINC 629 Left</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ARINC 629 Center</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ARINC 629 Right</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Fault Tolerant ADIRU

- Interconnections
  - FCMs communicate via serial busses
    » this keeps hardware complexity to a minimum
  - Power distribution
    » there are 3 robust power busses
    » the power of all 3 power supplies is summed for each bus
    » each FCM has own regulator
    » fault isolation keeps regulator failures independent
  - ADIRU transmits on 2 of 3 channels (left, right)
  - ADIRU receives on all 3 channels
  - 3rd channel used for SAARU (Secondary Air data Attitude Reference Unit)
Fault Tolerant ADIRU

- **Processor FCA**
  - contains fault tolerant clock (FTC)
  - used for 100 Hz synchronization interrupts providing processor synchronization

- **ARINC 629**
  - failures in any ARINC 629 bus are independent
  - votes on processor output before transmitting on bus
  - watchdog timers and power monitors are used to assure graceful shutdown if processor control over ARINC 629 interface is lost.
Fault Tolerant ADIRU

*Power supply*
- 3 supplies
- each has independent inputs for +28VDC primary power and +28VDC battery backup
- outputs are summed to produce single source of power (used by the 3 power busses)
- each supply employs
  » over-voltage monitoring
  » shut-down circuitry in case of power surge
  » under-voltage is not problem due to the power summing
Fault Tolerant ADIRU

- Redundancy management
  - Hardware data-consistency-checks used to provide same input to all processors.
  - Fault-tolerant detection and isolation software manages gyros and accelerometers.
    - "tries to eliminate benign faults"
  - Outputs from processors are voted on by the ARINC 629 interfaces.
  - Power supplies are mainly tested upon power-up and shut down for deferred maintenance.
Fault Tolerant ADIRU

- Fault Isolation
  - Design objectives are to maximize fault independence.
  - Electrical fault isolation
    » important since time to repair might be long
  - Mechanical fault isolation
    » shorts caused by foreign objects
  - Occams raiser approach: keep things simple.
  - Multiple methods (layers) of fault isolation
    » at least 2 levels to protect interfaces between FCMs
    » serial busses and discrete interconnections via isolation resisters on both ends
Fault Tolerant ADIRU

- Reliability
  - Typical Inertial Reference Unit
    » Mean Time Between Failure (MTBF)
      ■ typical 10,000 h
    » Mean Time to First Failure (MTFF)
      ■ typical 8,000 h
    » using TMR: MTBF = 10,000/3 = 3,333h
  - Deferred Maintenance Approach
    » Mean Time to Dispatch Alert with no maintenance
      ■ > 25,000h
      ■ assuming 1 fault sustained in each FCA
    » With better maintenance, i.e. fix unit at convenient time after annunciation
      ■ Mean Time to Dispatch Alert = 300,000h