Boeing 777

- Boeing 777 Primary Flight Computer
  - Paper: *Triple-Triple Redundant 777 Primary Flight Computer*
    - Y.C. Yeh
    - 1996 IEEE Aerospace Applications Conference
    - pg 293-307

Boeing 777

- Primary Flight Control Surfaces

Yeh96 fig.1
Boeing 777

- Overview
  - Flight control system is a *Fly-by-Wire* (FBW) system.
  - Delayed Maintenance for major electronic Line Replacement Units (LRU)
  - Triple redundancy for all hardware
    - computing system
    - airplane electrical power
    - hydraulic power
    - communication paths
  - Primary Flight Computer (PFC) are the central computational elements of the FBW system.
  - PFC architecture is based on TMR

- N-version dissimilarity integrated into TMR
  - 3 similar channels
  - each channel has 3 dissimilar computation lanes
  - software written in ADA (dissimilar compilers)
- DATAC bus, also known as ARINC 629 bus, is used for all communication between all computing systems for flight control functions.
  - DATEC = Digital Autonomous Terminal Access Communication
  - designed by Boeing
  - busses are isolated (physically and electrically)
  - DATA Cs are not synchronized
  - http://www.arinc.com
**Boeing 777**

- **777 FBW design philosophy**
  - Considerations
    - common mode/common area fault
    - separation of FBW components
    - FBW functional separation
    - dissimilarity
    - FBW effect on the structure
  - Triple-dissimilarity for PFC processors and interface hardware
  - By nature of TMR no Byzantine faults allowed.
  - Avoidance of asymmetry by:
    - ARINC629 requirements
    - Deal with root causes of functions/communication asymmetry

**Boeing 777**

- **Flight Control Functions**
  - Control electric and electro-hydraulic actuators
  - Provide manual and automatic control in pitch, roll and yaw axes
  - Control pilot input: column, wheel, rudder pedals, speed brakes
  - Pitch Control: 2 elevators and horizontal stabilizer
  - Roll Control: 2 ailerons, 2 aperons, 14 spoilers
  - Jaw Control: tabbed rudder
Three operation modes:

<table>
<thead>
<tr>
<th>CONTROL MODE</th>
<th>PITCH</th>
<th>ROLL</th>
<th>YAW</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL CONTROL</td>
<td>CONTROL: CT Manoeuvre Cond with Speed Feedback</td>
<td>CONTROL: Surface Cond Manual Trim Fixed Feel</td>
<td>CONTROL: Surface Cond &amp; HI Cap &amp; Thrust Asymmetry Compensation</td>
</tr>
<tr>
<td></td>
<td>Manual Trim for Speed Variable Feel</td>
<td>ENVELOPE PROTECTION Unit Angle</td>
<td>AUTONOMOUS</td>
</tr>
<tr>
<td></td>
<td>ENVELOPE PROTECTION</td>
<td>AUTOPILOT</td>
<td>AUTOPILOT</td>
</tr>
<tr>
<td></td>
<td>AUTOPILOT Endurance</td>
<td>Rudder</td>
<td>kehr Integrated</td>
</tr>
<tr>
<td>SECONDARY CONTROL</td>
<td>CONTROL: Surface Cond (Augmented)</td>
<td>CONTROL: Surface Cond Manual Trim Fixed Feel</td>
<td>CONTROL: Surface Cond, Flaps Up/Down Gain</td>
</tr>
<tr>
<td></td>
<td>Direct Stick/Trim</td>
<td>FIXED Feel</td>
<td>Pitch, Roll</td>
</tr>
<tr>
<td></td>
<td>Flaps Up/Down Feel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIRECT CONTROL</td>
<td>CONTROL: Surface Cond (Augmented)</td>
<td>CONTROL: Surface Cond Manual Trim Fixed Feel</td>
<td>CONTROL: Surface Cond, Flaps Up/Down Gain</td>
</tr>
<tr>
<td></td>
<td>Pitch, Roll</td>
<td></td>
<td>Pitch, Roll</td>
</tr>
<tr>
<td></td>
<td>Direct Stick/Trim</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flaps Up/Down Feel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Boeing 777

Sequence of events:
1) Actuator Control Electronics unit (ACE)
   - Position transducers (mounted on each pilot controller) sense pilot commands for the ACE
     » two actuator controlled feel units provide variable feel for control column
     » mechanical feel units provide fixed feel for wheel and paddles.
   - ACE performs A/D conversion
   - Transmits signals to PFCs via redundant ARINC 629 buses

2) Primary Flight Computer
   - Receive inertial data from
     » Air Data Inertial Reference System (ADIRS)
     » Secondary Attitude and Air Data Reference Unit (SAARU)
     » ACE
   - Compute Control-Surface position commands
   - Transmit position commands back to ACE via ARINC 629 buses
Boeing 777

3) Actuator Control Electronics unit
- Receives digital command from PFC
- D/A conversion
- Control electro-hydraulic actuators of control surfaces
- In Direct Mode, the ACEs use the analog pilot controller transducer signals to generate surface commands

- Line Replacement Unit (LRU)
  - PFC and ACE are the major LRU, connected via ARINC 629 buses

Boeing 777

- Actuator Control Electronics (ACE)
  - 4MR configuration
  - Interface between analog domain, e.g. crew controllers, electric/electro-hydraulic actuators, and digital domains, e.g. ARINC 629, PFCs
  - Controls all control surfaces
  - Controls variable feel actuators
  - 3 ARINC 629 interfaces
  - In Direct Mode commands on the digital bus are ignored => Provide direct surface control
Butterfly 777

- ACE overview

Yeh96 fig. 3
Boeing 777

- Primary Flight Computer (PFC)
  - TMR configuration
  - Receive data on all 3 ARINC 629 buses
  - Transmit on only one ARINC 629 bus
  - Each PFC contains 3 internal computation lanes
  - Each lane accesses all 3 buses
  - Each lane has dissimilar processors
  - Different Ada compilers

Boeing 777

- Primary Flight Computer

Yeh96 fig.5
**Boeing 777**

- ARINC 629 Digital Data Bus
  - time division multiplex system, up to 120 users
  - terminal access is autonomous, terminal listens, waits for quite period and transmits

3 protocol timers
insure fair access in round robin fashion

---

---
Boeing 777

- ARINC 629 bus requirements:
  - data bus availability requirements
  - tolerance to error occurrences of 1 in \(10^8\) bits
  - tolerance of aperiodic bus operation
  - transmission requirements to provide indication of output data freshness
    and to not output split-frame data
  - common CRC algorithm

Forward path signal monitor (Yeh96 fig.8)
Boeing 777

- Common Mode & Common Area Fault
  - Component and functional separation. Resistant to
    » maintenance crew error or miss-handling,
    » impact of objects, electric faults, electric power failure, electro-magnetic
      environment, lightning, hydraulic failure, structural damage
  - Separation of components
    » multiple equipment bays
    » physical separation, (including wiring)
    » separation of electrical and hydraulic line routing

Boeing 777

- Functional Separation
  » Left, Center, Right flight control electrical buses
  » Unit transmits on only 1 ARINC 629,
    ■ each unit transmits on its dedicated bus, but monitors the others
    ■ unit failure can effect only single bus
  » Distribution of actuator control,
    ■ i.e. L/C/R units control actuators using L/C/R respective buses.
- Dissimilarity
  » dissimilar microprocessors
  » dissimilar compilers
  » dissimilar control & monitor functions
  » dissimilar inertial data systems
  » ACE direct mode allowing bypassing of buses
Boeing 777

Safety Requirements
- PFC: probability of $10^{-10} / h$
  - functional integrity (active failures affecting plane structure)
  - functional availability (passive failures)
- $10^{-10} / h$
  - all PFC operational
  - any single lane fault
- $10^{-10} / h$ per auto-landing operation for:
  - full operational system
  - single lane fault in any/all PFC
  - single PFC fault
  - single PFC fault & multiple single lane faults
- No single fault should cause error without failure indication
- No single fault should cause loss of > 1 PFC

Redundancy Management
- PFC inter-lane communication within each PFC channel
- Frame synchronization
- (Input) Data synchronous operation
- Median value selection
- Cross-Channel Consolidation and Equalization
- PFC external resource monitoring
- In addition to ARINC bus: private cross-lane data bus for
  - frame synchronization within a PFC channel
  - data synchronization within a PFC channel
  - cross-lane data transfer
Redundancy Management: typical control path

PFC lane redundancy management
Boeing 777

* Synchronization
  - Frame Synchronization
    - to allow tight cross-lane monitoring
    - convergent (mid-point selection) frame synchronization
    - tight synchr. within a few microseconds (what about worse case?)
  - Data Synchronization
    - 2 MHz ARINC 629 => transmit duration > 20us
    - 20us >> frame synchronization time, thus giving sufficient time for data synchronization
    - all PFC lanes are synchronized to the same data set.
      - this data is then used at the beginning of each computation frame
      - allows tighter tracking between lanes
    - occasional PFC lane differences are tolerated

Boeing 777

* Monitoring
  Dual role of PFC lanes
  - Command role:
    - only one lane
    - will send proposed surface command to ARINC 629
    - output is result of median select
    - other ARINC 629 receive command from other PFCs
  - Monitor role:
    - “selected output” monitoring
    - cross-line inhibit hardware logic
  - Cross-Line and Cross-Channel monitoring
  - Critical discretes and variables are equalized between PFC channels