Boeing 777 Triple Triple
Redundant Flight Controller
Boeing 777
Table of Contents

☐ General Remarks/Scope
☐ Features and Technologies of Boeing 777
☐ Primary Flight Controller
  ▪ Overview
  ▪ Control Modes
  ▪ Safety Design Constraints
  ▪ Safety Requirements
  ▪ Architecture
☐ AIMS Robust Computing Architecture
☐ Validation and Verification Process
☐ Outlook
☐ Sources
Boeing 777 Flight Controller
General Remarks / Scope

☐ Restriction on sources due to commercial interests
  - Not all details known
  - Contradictory statements in different sources

☐ Use of existing technologies
  - ARINC 629 data bus
  - Frame Synchronization
  - Lynx and CsLEOS RTOS
  - ADA Programming Language
Boeing 777 Flight Controller

Features

- Long-range and high density market
  - Serious rival to Airbus A330 and A340
  - Twin-Engine
  - 350-450 seat market
  - Cargo Capacity
  - IFE/PTV in Y Class

- 777-200LR: LHR->SYD Nonstop
  - Constraint: only eastbound with tailwinds in about 20h

- Built in Everett, WA

- First commercial flight in 1995

- Important Costumers
  - UAL, ANA, JAL, BA, Singapore Airl., Emirates, ILFC and even Air France, but not LH

- Price: USD 165m to 250m a piece
777 Primary Flight Controller Technologies

- Fly-By-Wire (FBW)
  - 100% Electronic Flight control system
    - Boeing to catch up with Airbus (Airbus A320)
  - Primary Flight Controller (PFC)
  - Automatic Landing

- Airplane Information Management System (AIMS)
  - Navigational aid, flight indicator
Boeing 777
Table of Contents

☐ General Remarks/Scope
☐ Features of Boeing 777
☐ Primary Flight Controller
  ▪ Overview
  ▪ Control Modes
  ▪ Safety Design Constraints
  ▪ Safety Requirements
  ▪ Architecture
☐ AIMS Robust Computing Architecture
☐ Validation and Verification Process
☐ Outlook
☐ Sources
777 Primary Flight Controller
Overview

- **Triple Triple Redundancy (TMR) for all hardware resources**
  - Triple channels with triple dissimilar lanes in each channel
  - Computing system, electrical power, hydraulic power, communication path (not engines!)

- **Fly-By-Wire (FBW) Flight Control System for Boeing 777**
  - No heavy mechanical cables
  - Powered by three GEC-Marconi primary flight control computers (132k LOC Ada, with 3 different ADA compilers for triple dissimilarity)
  - Deferred Maintenance

- **Central Computing Element: Primary Flight Controller (PFC)**
  - E.g. calculating control surface position commands
  - FBW to provide manual and automatic control of electrohydraulic actuators (using electrically transmitted command) of pitch, roll and yaw axes
777 Primary Flight Controller Overview

- A/D conversion with ACE’s (Actuator Control Electronics)
- Data transmission via DATAC bus (ARINC 629)
  - TDM, 2 MBits/s, one wordstring in 20 ms
  - 120 users (connecting to bus with coupler, one transmission by one terminal at a time in defined time intervals)
  - Terminal Controller
    - Demodulator used for checking faults
    - Receiver Circuitry determines which data needed
    - Subsystem Interface
- PFC Cross-Channel and Cross-Lane Data Bus
  - Frame Synchronization
  - Data Synchronization
  - Median Value
Three PFC’s to provide triple redundant computational channels

- Three internal computational lanes
- Receiving data from three data buses (transmitting only to one bus) via ARINC 629 terminals
Time division multiplex ARINC 629 data bus
777 Primary Flight Controller
Control Modes

<table>
<thead>
<tr>
<th>Control Mode</th>
<th>PITCH</th>
<th>ROLL</th>
<th>YAW</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL MODE</td>
<td>□ Control</td>
<td>□ Control</td>
<td>□ Control</td>
</tr>
<tr>
<td></td>
<td>□ C* Maneuver Cmd with Speed Feedback</td>
<td>□ Surface Cmd (Augm.)</td>
<td>□ Surface Cmd (Augm.), Wheel/Rudder Gross Tie</td>
</tr>
<tr>
<td></td>
<td>□ Envelope Protection</td>
<td>□ Manual Trim</td>
<td>□ Fixed Feel</td>
</tr>
<tr>
<td></td>
<td>□ Stall, Overspeed</td>
<td>□ Fixed Feel</td>
<td>□ Yaw Rate Damper</td>
</tr>
<tr>
<td></td>
<td>□ Autopilot</td>
<td>□ Yaw Rate Damper</td>
<td>□ Gust Suspension</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Envelope Protection</td>
<td>□ Thrust Asymmetry Compensation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Autopilot</td>
<td>□ Autopilot</td>
</tr>
<tr>
<td>SECONDARY MODE (Boeing 747)</td>
<td>□ Control</td>
<td>□ Control</td>
<td>□ Control</td>
</tr>
<tr>
<td></td>
<td>□ Surface Cmd (Augm.)</td>
<td>□ Surface Cmd (Augm.)</td>
<td>□ Surface Cmd (Augm.), PCU Pressure Reducer</td>
</tr>
<tr>
<td></td>
<td>□ Flaps Up/Down Gain</td>
<td>□ Manual Trim</td>
<td>□ Fixed Feel</td>
</tr>
<tr>
<td></td>
<td>□ Direct Stabilizer Trim</td>
<td>□ Fixed Feel</td>
<td>□ Yaw Rate Damper</td>
</tr>
<tr>
<td></td>
<td>□ Flaps Up/Down Feel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIRECT CONTROL (mechanical link)</td>
<td>□ Control</td>
<td>□ Control</td>
<td>□ Control</td>
</tr>
<tr>
<td></td>
<td>□ Surface Cmd (Augm.)</td>
<td>□ Surface Cmd (Augm.)</td>
<td>□ Surface Cmd (Augm.), PCU Pressure Reducer</td>
</tr>
<tr>
<td></td>
<td>□ Flaps Up/Down Gain</td>
<td>□ Manual Trim</td>
<td>□ Fixed Feel</td>
</tr>
<tr>
<td></td>
<td>□ Direct Stabilizer Trim</td>
<td>□ Fixed Feel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>□ Flaps Up/Down Feel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Switch to Direct Mode if ACE‘s to detect invalid commands from PFC
- Analog pilot controller transducer signals for surface commands
- ACE not to respond to ARINC 629 data bus

Switch to Secondary Mode if detecting insufficient air data or ACE‘s in direct mode

Mode Switching is open to discussion
Primary Flight Controller
Safety Design Constraints

- Common mode/ common area faults
- Separation of concerns for FBW (LRU) components
- FBW functional separation
- Dissimilarity
- FBW effect on structure
Common mode/ common area faults

- Impact of objects
- Structural damage
- Electrical faults
- Lightning strike
- Hydraulic failure
- Pilot error
□ Separation of FBW Hardware Units

- Isolation
- Separation of electrical and hydraulic line routing through airplane structure
- Flight deck equipment and wiring separation and protection from foreign object collision
- Multiple Equipment Bays LRU (Line Replaceable Units)
Primary Flight Controller
Safety Design Constraints

☐ Functional Separation
  - (L)eft, (C)enter, (R)ight positions of hardware resources
    - Electrical power, flight control ARINC 629 buses, PFCs, ACEs, Hydraulic systems
    - PFC’s and ACE’s to listen to all 3 ARINC 629 channels
    - L/C/R PFC’s and ACE’s to transmit to corresponding L/C/R ARINC 629 channel only
Primary Flight Controller
Safety Design Constraints

Figure 4  777 Primary Flight Controls: Hydraulic / ACE Distribution
Primary Flight Controller
Safety Design Constraints

☐ Dissimilarity

- Design errors to defeat redundant strategies
- Dissimilar design
- Dissimilar Microprocessor (AMD, Motorola, Intel, ADA Compilers)
- ACE Dissimilar Control and Monitor Functions
  - Bypassing ARINC 629 by private bus
- N-Version programming
Primary Flight Controller
Safety Design Constraints

- FBW effect on structure
  - Envelope Protection
Primary Flight Controller
Safety Requirements

☐ Single fault not to lead to erroneous transmission of output signal without failure indication

☐ Single fault not to result in loss of function in more than one PFC

☐ Fail-Passive and Fail-Operational Electronics
  ▪ "An electronics function is fail-passive if, in the event of a failure, the continued safe flight and landing of an airplane can be maintained by the pilot"
Primary Flight Controller Architecture

- **PFC Cross-Lane Data Bus**
  - Private Bus apart from ARINC 629
  - Frame and Data Synchronisation within a PFC channel
    - For tight tracking/monitoring of each lane
  - Cross-Lane data transfer to complement other PFC (redundancy)

- **Input Data synchronous operation within each PFC channel**
Primary Flight Controller Architecture

- **Median Value Select for PFC output commands**
  - Performed by command lane after calculating surface commands
  - Fault blocking through Cross-Lane-Monitoring and lane inhibition via hardware logic

- **PFC external resources monitoring**
  - Terminal Controller (Demodulator, Receiver, Subsystem Interface)
  - PFC Cross-Channel Consolidation and Equalization
    - Channel Output Select Function (Terminal Controller)
    - Channel inhibition
  - Annunciation of marginal errors to AIMS
Boeing 777
Table of Contents

☐ General Remarks/Scope
☐ Features and Technologies of Boeing 777
☐ Primary Flight Controller
  ▪ Overview
  ▪ Control Modes
  ▪ Safety Design Constraints
  ▪ Safety Requirements
  ▪ Architecture
☐ AIMS Robust Computing Architecture
☐ Validation and Verification Process
☐ Outlook
☐ Sources
Airplane Information Management System
Overview

- AIMS (Airplane Information Management System) by Honeywell
  - Consists dual cabinets with all central processing, I/O hardware needed for flight management, flat-panel cockpit displays
  - Condition monitoring
  - AIMS replaceable units not self-contained
    - Functions gathered in AIMS share processors, memory system, hardware, I/O ports (out of economic reason)
  - AIMS communicates with 777 components through 12 data bus networks (11 Arinc 629, 1 optical fiber)
Digital Processor with elements for rapid recovery

- Self-checking pairs processor with Honeywell SAFEbus communication technology
  - Detecting loss of output by master
    - If faulted processor module, two copies of processor „state data“ in core
  - Within nanoseconds faulty unit is blocked from generating output

AIMS can be dispatched with one failed processor or failed I/O module
Boeing 777
Table of Contents

- General Remarks/Scope
- Features and Technologies of Boeing 777
- Primary Flight Controller
  - Overview
  - Control Modes
  - Safety Design Constraints
  - Safety Requirements
  - Architecture
- AIMS Robust Computing Architecture
- Validation and Verification Process
- Outlook
- Sources
Boeing 777 Flight Controller
Validation and Verification Process

- Testing of actuating in B757 “Iron Bird” (SIL)
  - Contained most operational LRU's

- CATIA
  - 100% paperless airliner

- Error scenario
  - Single/dual engine out, single/dual hydraulics, sensor failures
  - Propagation

- ETOPS certification

- Problems in capturing requirements, chaotic change management (esp. with contractors) and detail trap
Boeing 777
Table of Contents

☐ General Remarks/Scope
☐ Features and Technologies of Boeing 777
☐ Primary Flight Controller
  ▪ Overview
  ▪ Control Modes
  ▪ Safety Design Constraints
  ▪ Safety Requirements
  ▪ Architecture
☐ AIMS Robust Computing Architecture
☐ Validation and Verification Process
☐ Outlook
☐ Sources
Boeing 777 Flight Controller
Outlook

- **Deferred Maintenance**
  - Improvement of airplane dispatch reliability (delays, delays)
  - Life Cycle Cost: Computer Architectures one level of redundancy beyond requirement

- **Operating System**
  - Lynx RTOS
  - CsLEOS Real-Time Operating System from BAE Systems

- **ADA Programming Language**

- **Boeing 787 Dreamliner**
Boeing 777
Table of Contents

- General Remarks/Scope
- Features and Technologies of Boeing 777
- Primary Flight Controller
  - Overview
  - Control Modes
  - Safety Design Constraints
  - Safety Requirements
  - Architecture
- AIMS Robust Computing Architecture
- Validation and Verification Process
- Outlook
- Sources

„Boeing‘s seventh Wonder“, IEEE Spectrum, 1995

Y.C. Yeh, „Design Considerations in Boeing 777 Fly-By-Wire Computers“, Boeing, Seattle

Y.C. Yeh, „Triple-Triple Redundant 777 Primary Flight Computer“, Boeing, Seattle


Thank You !!!

Photo Copyright © Tim de Groot - AirTeamImages