Ultra-Reliable Fly-By-Wire Computers for Commercial Airplanes' Flight Controls Systems

Ying Chin (Bob) Yeh, Ph. D., IEEE Fellow
Technical Fellow
Flight Controls Systems
Boeing Commercial Airplanes

IEEE ComSoc Technical Committee on Communication Quality & Reliability

Emerging Technology Reliability Roundtable

Tucson, AZ, USA, May 12, 2014

Ultra-Reliable Fly-By-Wire Computers for Commercial Airplanes' Flight Controls Systems

- Introduction: FBW Computers Chronological History & FAR
- Fail-Passive and Fail-Operational Avionics
- Fundamental Concept of Dependability
- Industry Experiences on Error Types
- Boeing FBW Design Philosophy for Safety
- 777 FBW Requirements and Design Philosophy
- Common Mode Failure and Single Point Failure
- Generic Error and Dissimilarity Considerations
- Safety Requirements for 777 FBW Computers

High Level Chronology of High Integrity Computing

Academic & NASA	Year	Industry
First Computer Developed at U Penn	**1947**	
Professor Shannon (MIT): Building Reliable Systems with Un-reliable components	**1950**	Bell Labs ESS (Electronic Switching System)
Information Theory & Coding (Error detection & correction, Hamming code, etc)		IBM Main Frame Computer (with fault tolerance concept)
NASA Space Program	**1960**	Bell Systems Undersea Cable (Electronics and system design for high reliability)
		Boeing Flight Controls C* Handling Quality Criterion developed
IEEE International Conference on Fault Tolerant Computing Started	**1970**	Military FBW (Fly-By-Wire) Systems
NASA-Langley FBW Program, 1972 - 78 (Draper Lab, SRI International)		Military Data Bus (1553 protocol)
Space Shuttle FC Computer		Boeing Linear Data Bus R&D for FBW (ARINC 629)
IEEE/IFIP Dependable Systems and Networks	**1980**	Boeing Commercial Airplane FBW R&D, 1984 -
		Bell Labs No. 5 ESS
		First Commercial Airplane FBW (A320), 1988
	1990	Boeing 777 FBW, 1995
		EU Drive-by-Wire
		Embraer-170 FBW (Analog)
	2011	Boeing 787 FBW
	2017	China 919 FBW (projected)
NASA (next) Moon Landing	**20XX?**	

Harmonized FAR 25.1309 Requirements

Harmonized 25.1309 Requirements and Compliance Summary					
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
DO-178B S/W & DO-254 H/W Levels	Level E	Level D	Level C	Level B	Level A
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Allowable Quantitative Probability:	10-3 / 10-5 / 10-7 / 10-9 Average Probability per Flight Hour (or per Flight if Less than One Hour) on the Order of:				
System Compliance Method (Common cause hazards not conducive to numerical analysis, such as foreign object collision, human error, etc. may be analyzed primarily by Design Review.)	FHA & Design Review Design, functional separation, and implementation reviewed to ensure failures will only produce no safety effect.	FHA & Design Review Design, functional separation, and implementation reviewed to ensure failures will only produce Minor effect.	FHA, Design Review, & FMEA Review Failure modes & effects analysis reviewed to ensure that failure effects of components involved in the function and failure rates are appropriate for Major category	FHA, Design Review, & Fault Tree Analysis FMEA & FHA data combined in detailed fault tree analysis to validate that the system probability of hazard is Extremely Remote.	FHA, Design Review, & Fault Tree Analysis FMEA & FHA data combined in detailed fault tree analysis to validate that the system probability of hazard is Extremely Improbable
Effect Category Validation	All functional hazards should have a multi-disciplinary review by experts representing the engineering and operational areas. Where functions are the same as previous airplanes, past experience should be reviewed. Other conditions should be evaluated in lab and simulation tests. Failures affecting handling qualities will be evaluated in piloted simulation and/or flight test.				Specific failures may be evaluated by piloted simulation as necessary.

Fail-Passive and Fail-Operational

- Fail-Passive Electronics to avoid active airplane effect
  - An electronics function is said to be fail-passive if its failure effect is loss of its output for its intended function
- Fail-Operational Electronics via multiple redundant hardware
  - Multiple redundant hardware can facilitate meeting functional availability requirements for safety critical electronics system, as long as there exists no common-mode or single point failure.
- 777 FBW computers are used for elaboration

Fundamental Concepts of Dependability (Avizienis & Laprie & Randell)

- Among 4 classes of accidental or non-malicious faults,
  - Human-made interaction faults
  - Design faults
  - Physical internal faults
  - Physical external faults
- Human-made interaction and design faults dominate as sources of failure/error for larger, controlled systems

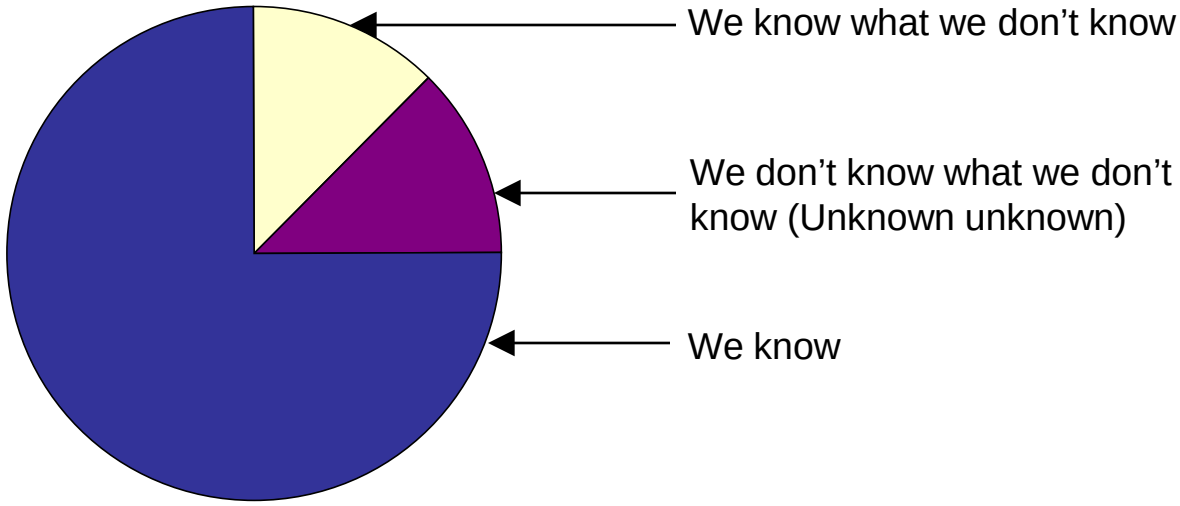
Flight Controls Industry Experiences on Error Types of Complex Flight Controls Systems

- Requirement Error*
- Implementation Misunderstanding*
- Software Design or Coding Error*
- Future Process Errors in Previously Qualified Electronics Parts
- Relatively new programmable VLSI circuits whose number of states approach infinity and therefore non-deterministic

**Can be attributed to Interaction Fault, Software/Hardware Interface Incompatibility*

Boeing FBW Design Philosophy for Safety

- *To meet extremely high functional integrity and functional availability requirements (of 1.0E-10 per hour), multiple redundant hardware resources are required for FBW systems.*
- *The fault tolerance for trustworthy FBW system design should consider all known and unknown causes of problem/failure/error, known as common mode failure and single point failure.*



777 FBW Requirement and Design Philosophy

The FBW requirements are developed from:

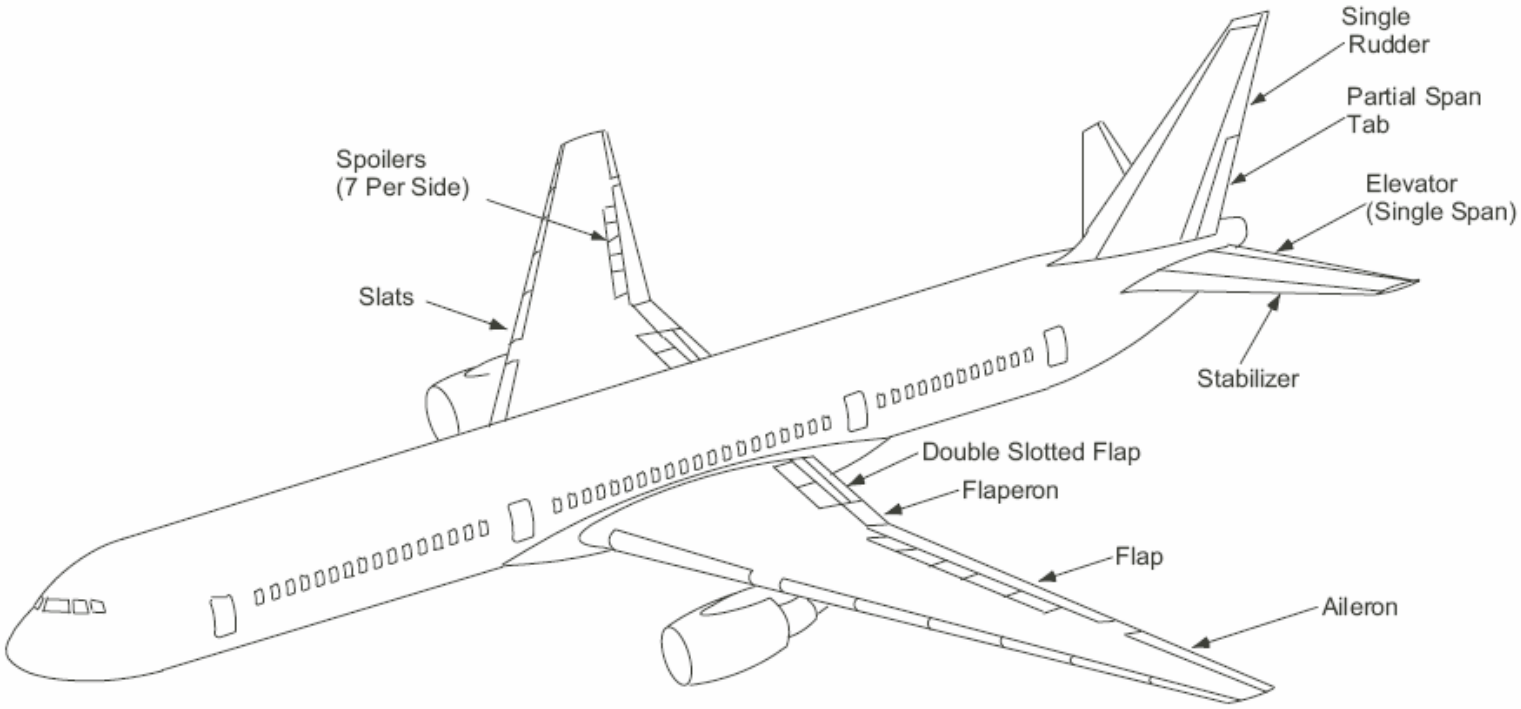
- Certification agencies requirements
- Customer and Boeing requirements

❖ Postulated failures, regardless probability of occurrences, can become derived requirements by a group of knowledgeable persons

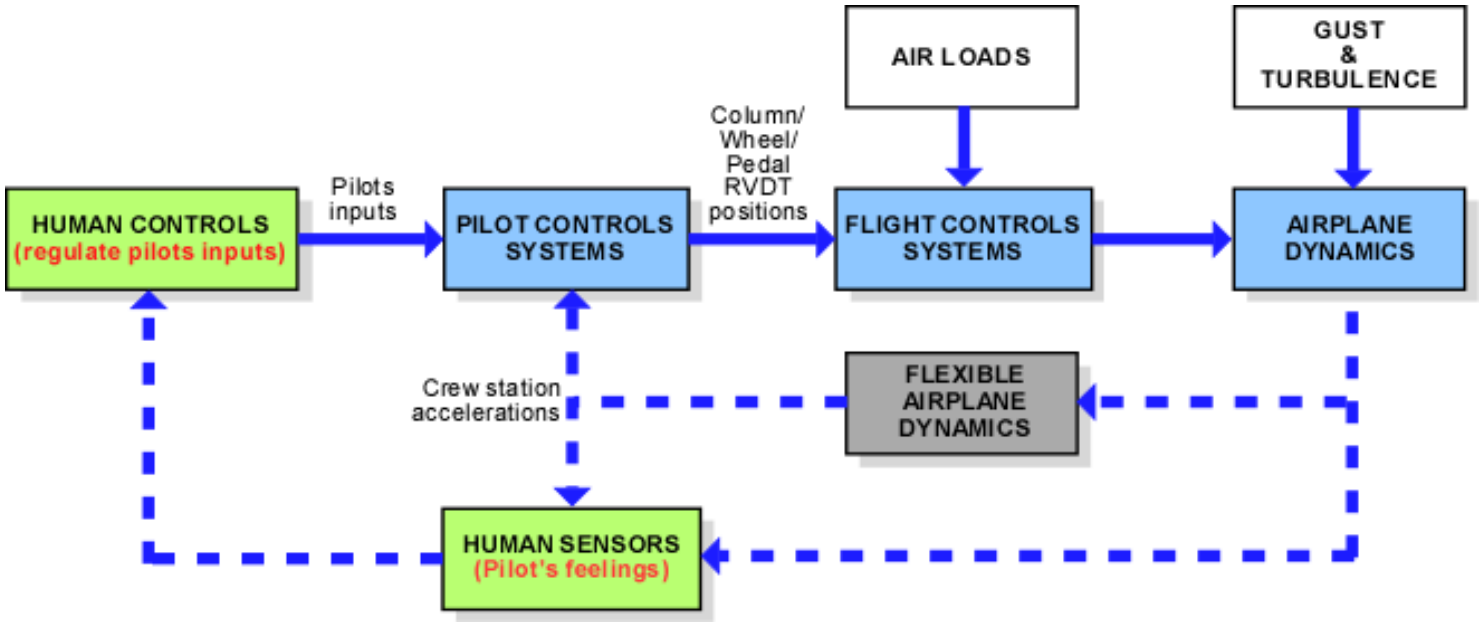
❖ Key FBW computer architectures per NASA FBW (FTMP/FTP, SIFT, MAFT): Byzantine Failure

❖ Derived 777 FBW design requirements for potential communication asymmetry and functional asymmetry

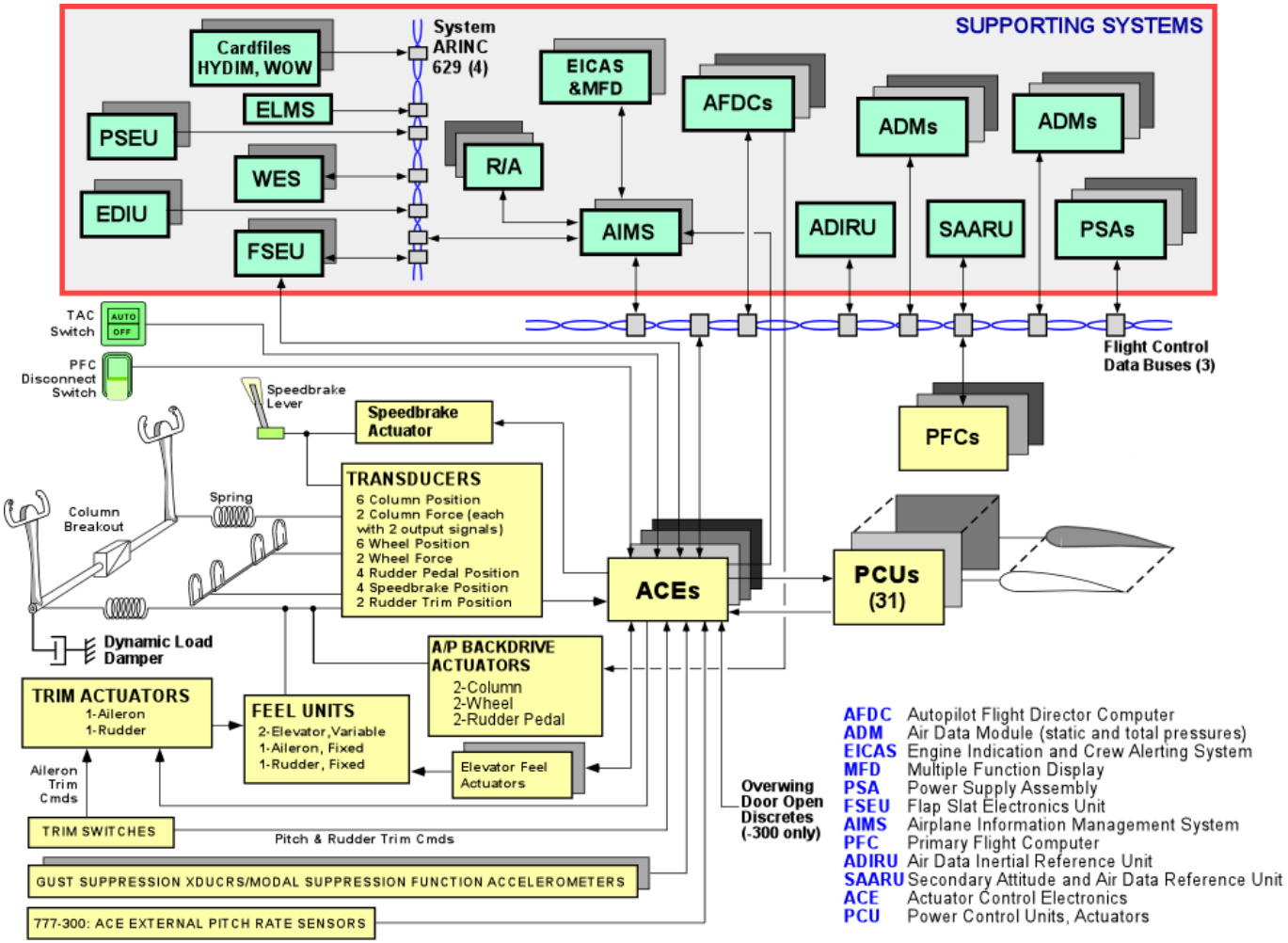
777 Control Surfaces



Airplane Control-Aerodynamics-Structure-Pilot Interactions Concept Diagram



777 Primary Flight Control System



Common Mode Failure (per SAE ARP4754)

- *Airplane susceptibility to common mode and common area damage is addressed by designing the systems to both component and functional separation requirements. This includes criteria for providing installations resistant to maintenance crew error or mishandling, such as:*
  - *Impact of objects*
  - *Electrical faults*
  - *Electrical power failure*
  - *Electromagnetic environment*
  - *Lightning strike*
  - *Hydraulic failure*
  - *Structural damage*
  - *Radiation environment in the atmosphere*
  - *Ash cloud environment in the atmosphere*
  - *Fire*
  - *Rough or unsafe installation and maintenance*

Dissimilarity of 777 FBW Electronics

PFC:

- Dissimilar processors and compilers (common software)
- DO-178 development process
- ASIC development process

ACE:

- Dissimilar monitor and control functions
- ASIC development process

Inertial Data:

- Dissimilar ADIRU/SAARU
- DO-178 development process

AFDC:

- DO-178 development process
- ASIC development process
- Dual dissimilar hardware for backdrive function

ARINC 629:

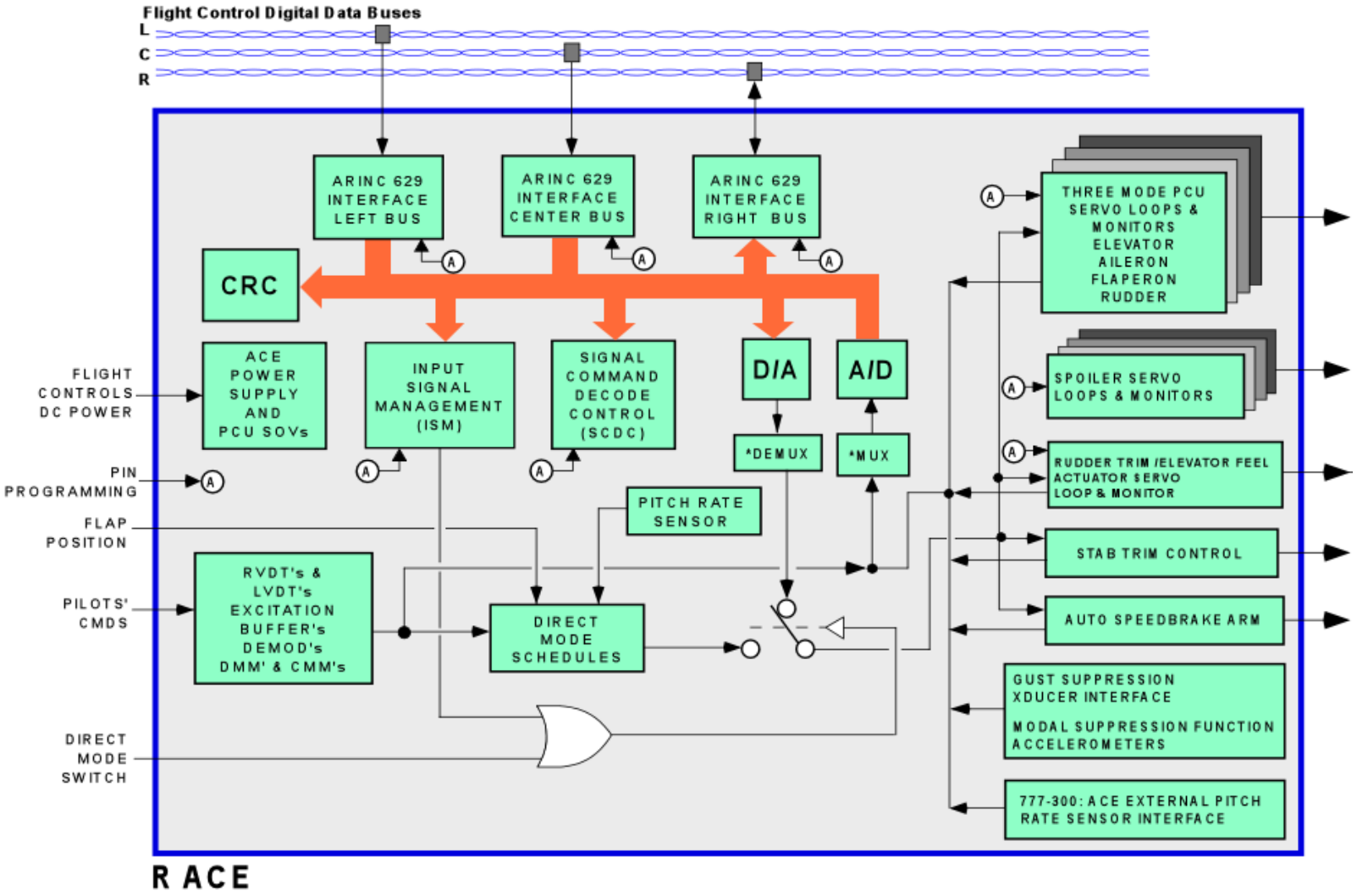
- ACE Direct Mode which bypass ARINC 629

777 PFC
Safety Requirements

- Numerical probability requirements
  - < 1.0E-10 per hour for functional integrity requirement
  - < 1.0E-10 per autoland during the critical phase of an autoland
  - < 1.0E-10 per hour for 777 PFC functional availability
- Non-numerical safety requirements

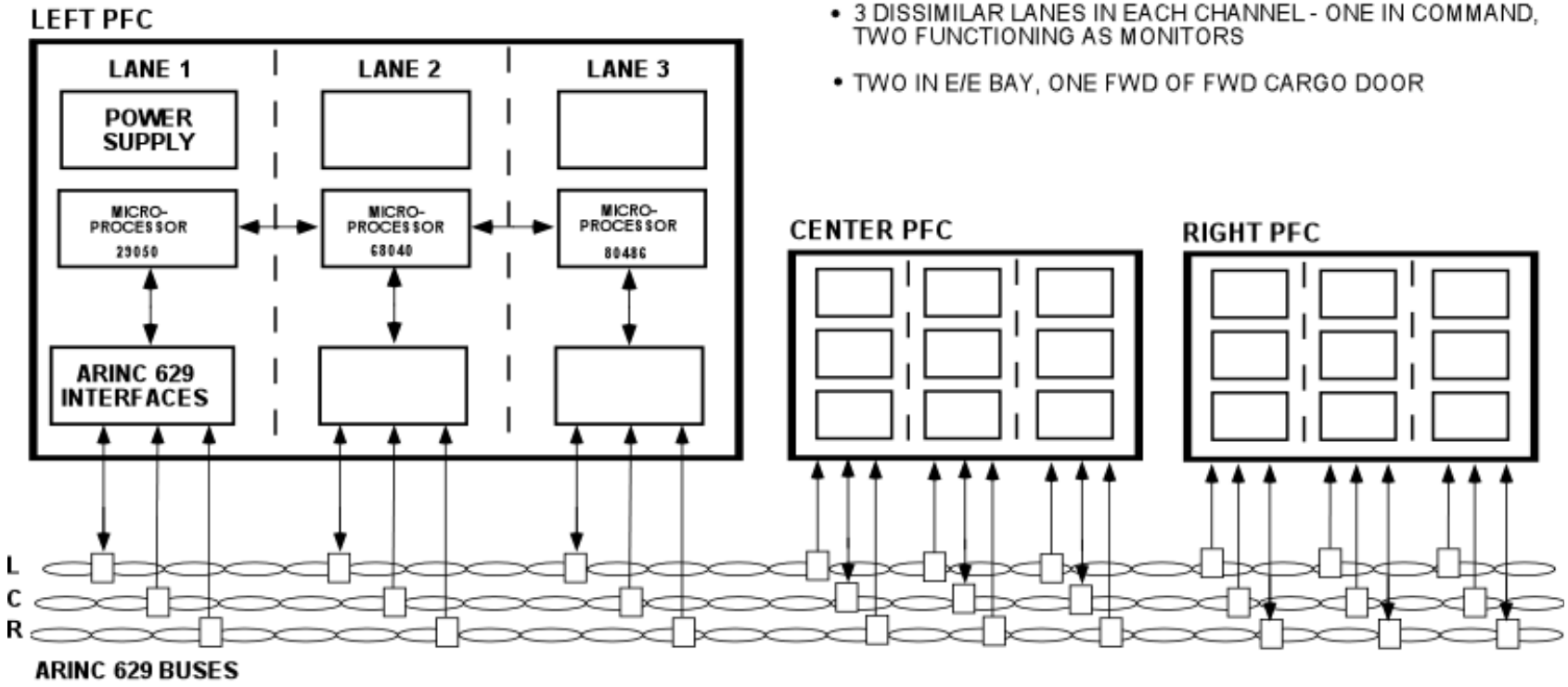
  No single fault, including common-mode hardware fault, regardless of probability of occurrence, shall result in:
  - An erroneous transmission of output signals without a failure indication.
  - Loss of function in more than one PFC

777 Actuator Control Electronics Architecture

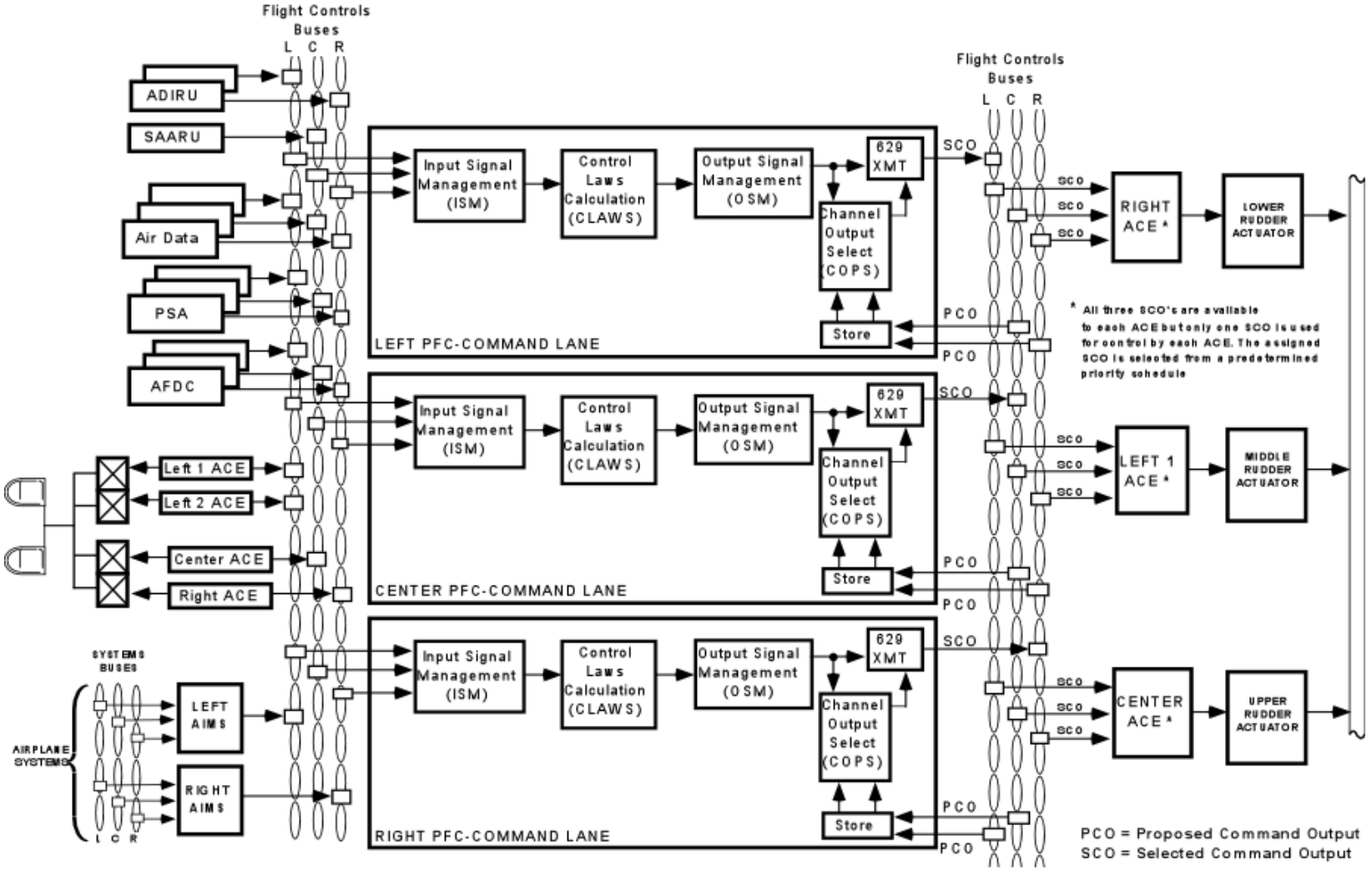


Triple-Triple Redundant
777 Primary Flight Computer

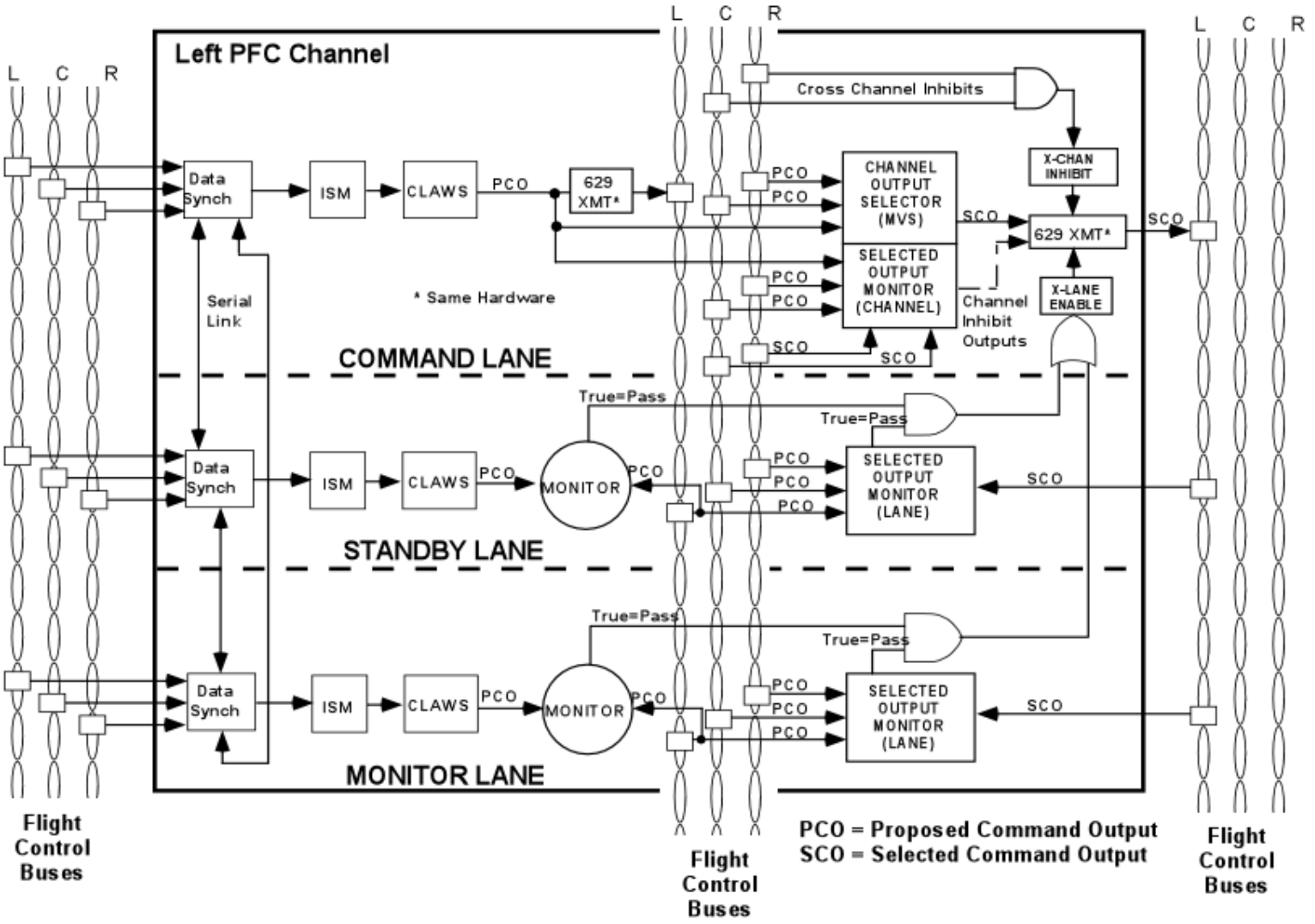
- 3 IDENTICAL CHANNELS - LEFT, CENTER, RIGHT
- 3 DISSIMILAR LANES IN EACH CHANNEL - ONE IN COMMAND, TWO FUNCTIONING AS MONITORS
- TWO IN E/E BAY, ONE FWD OF FWD CARGO DOOR



777 PFC Channel Command Path



777 PFC Channel Command/Monitor Architecture



777 PFC-ACE Signal Path