LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

JIM McWHA

CHIEF ENGINEER - FLIGHT CONTROLS

BOEING COMMERCIAL AIRPLANE GROUP

AUGUST 20, 1990

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

INDUSTRY STATUS

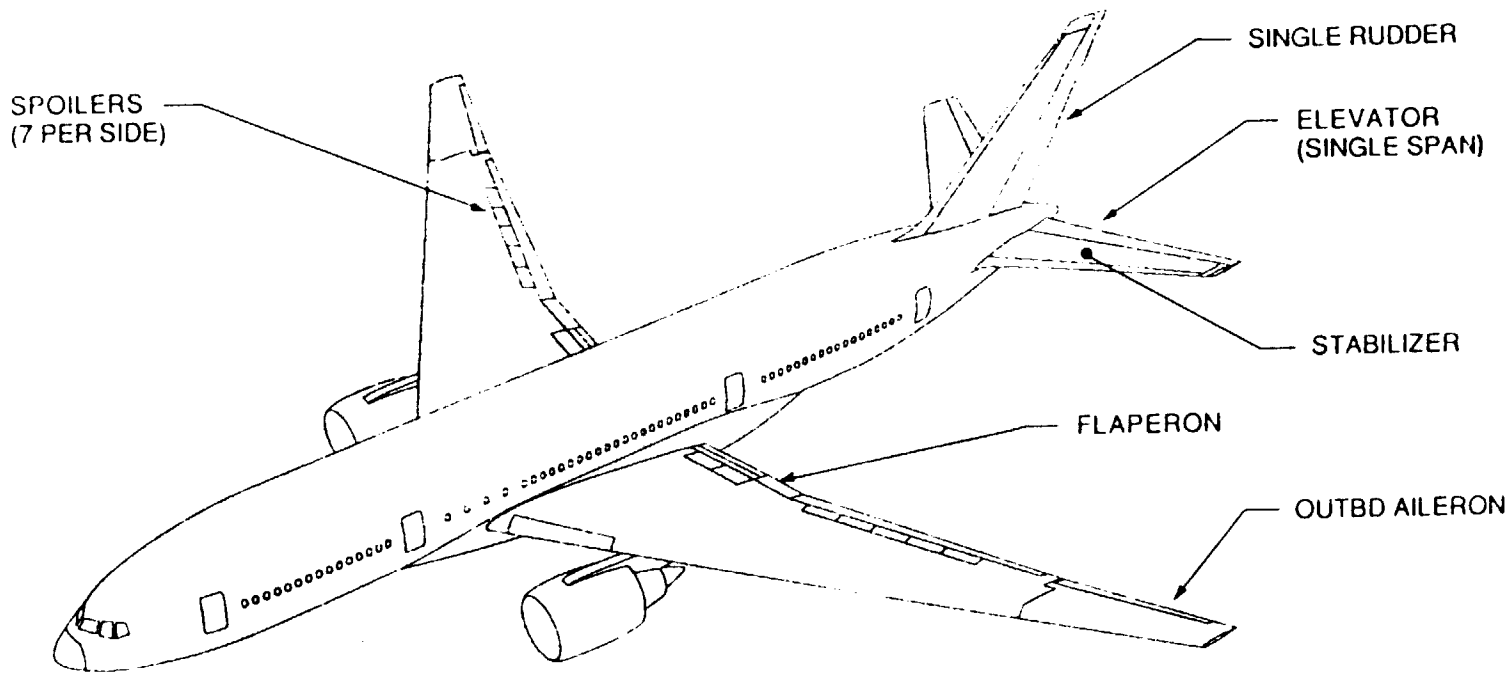
DIGITAL AUTOPILOT SYSTEMS WERE FIRST CERTIFICATED FOR USE ON COMMERCIAL AIRPLANES IN THE LATE 1970'S

THE A-320 AIRPLANE WAS THE FIRST COMMERCIAL AIR TRANSPORT AIRPLANE TO BE CERTIFICATED WITH A FLY BY WIRE PRIMARY FLIGHT CONTROL SYSTEM

BOEING WILL HAVE ALL FLY BY WIRE FLIGHT CONTROLS ON THE 767-X (777) AIRPLANE

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

- DEFINITION
- SAFETY
- INDUSTRY STATUS
- PROGRAM PHASES



767-X PRIMARY FLIGHT CONTROL SURFACES

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

DEFINITION

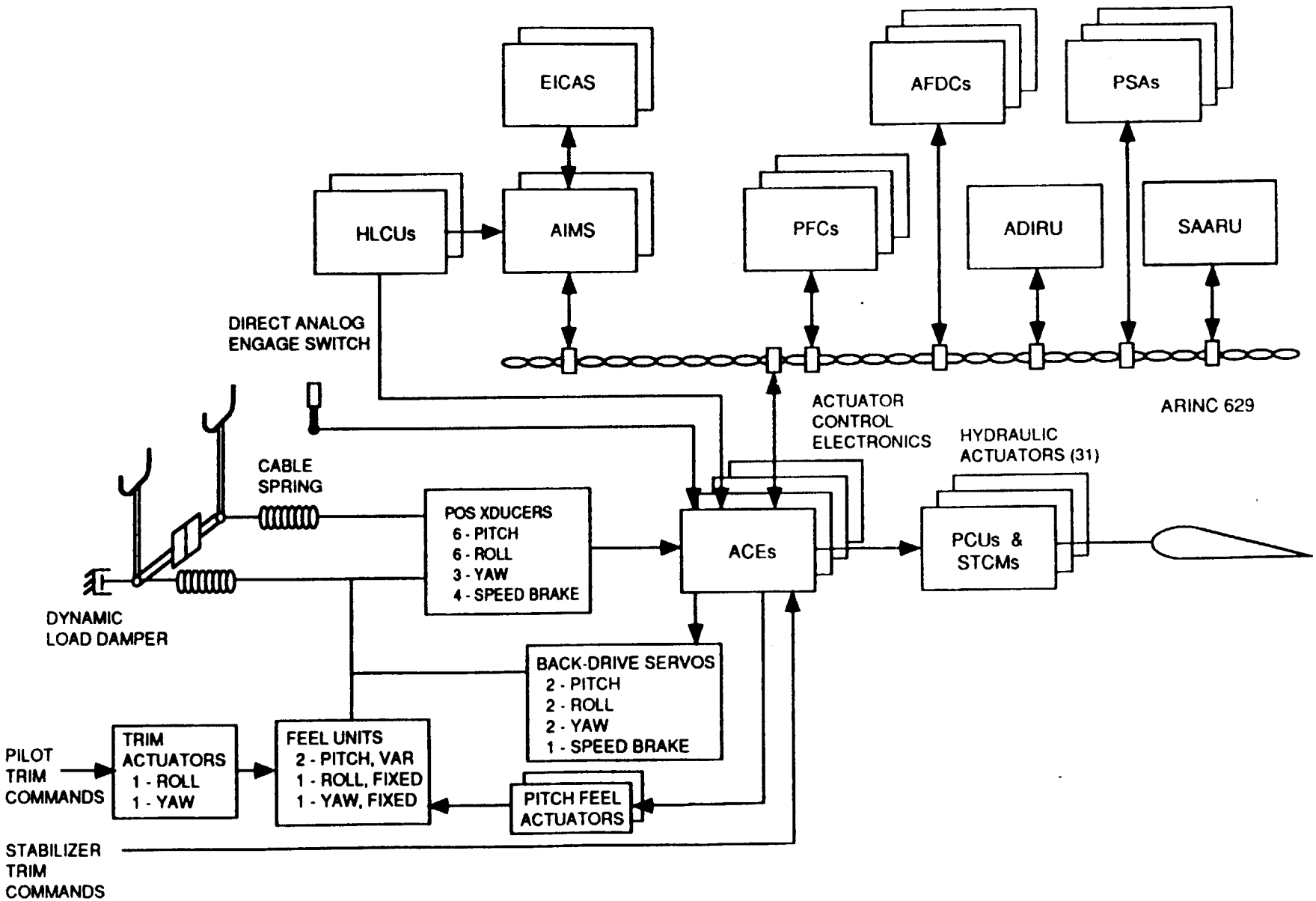
A CONTROL SYSTEM IMPLEMENTED IN DIGITAL COMPUTER TECHNOLOGY WHICH HAS A FUNCTION WHICH IF NOT PERFORMED AS INTENDED IS LIFE THREATENING

EXAMPLES: AN AUTOPILOT USED FOR AUTOMATIC LANDING IN LOW VISIBILITY CONDITIONS

AN AIRPLANE CONTROL SYSTEM IMPLEMENTED WITHOUT CONTROL CABLES:

FLY BY WIRE

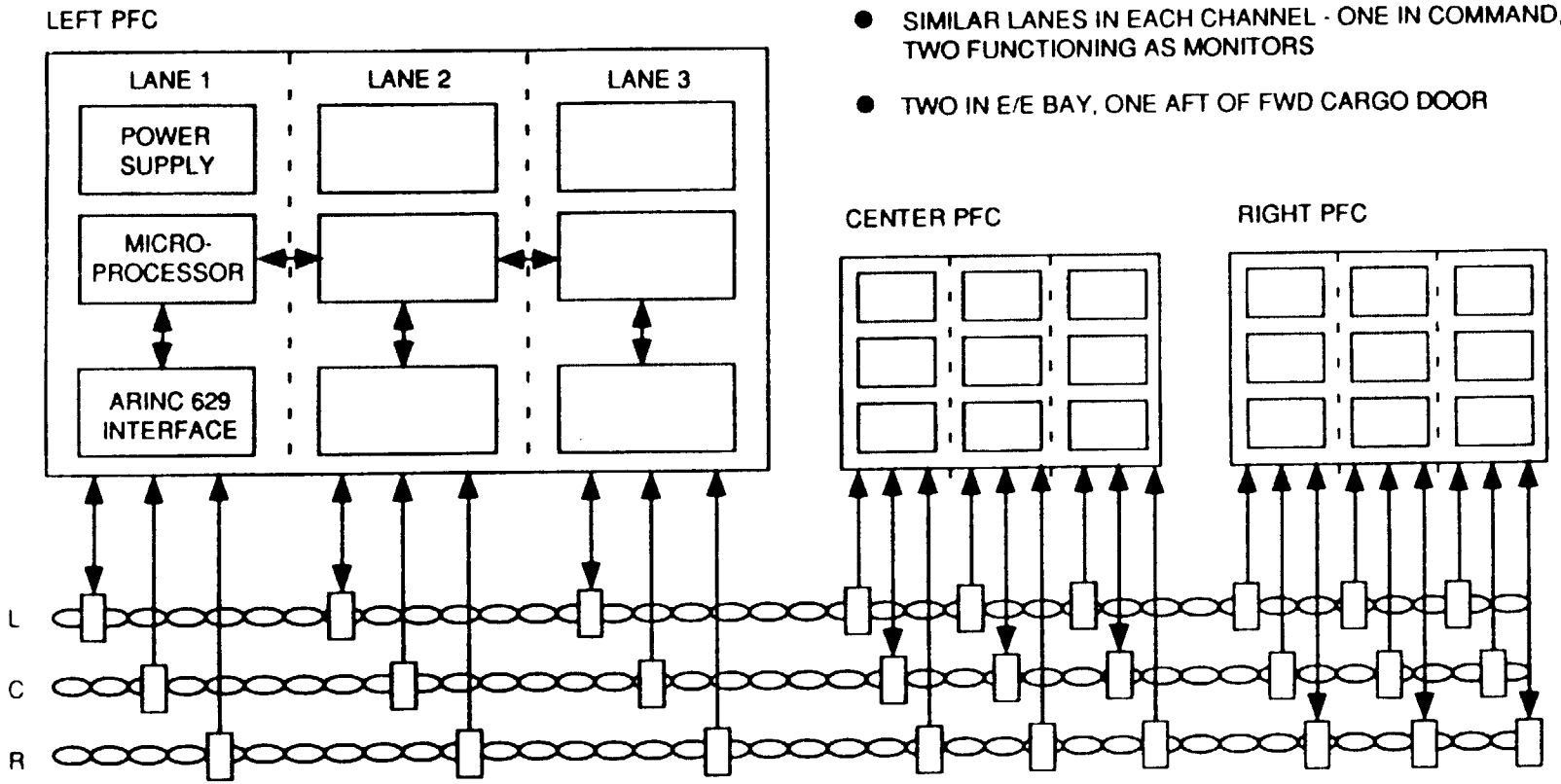
FLY BY LIGHT



767-X PRIMARY FLIGHT CONTROL SYSTEM OVERVIEW

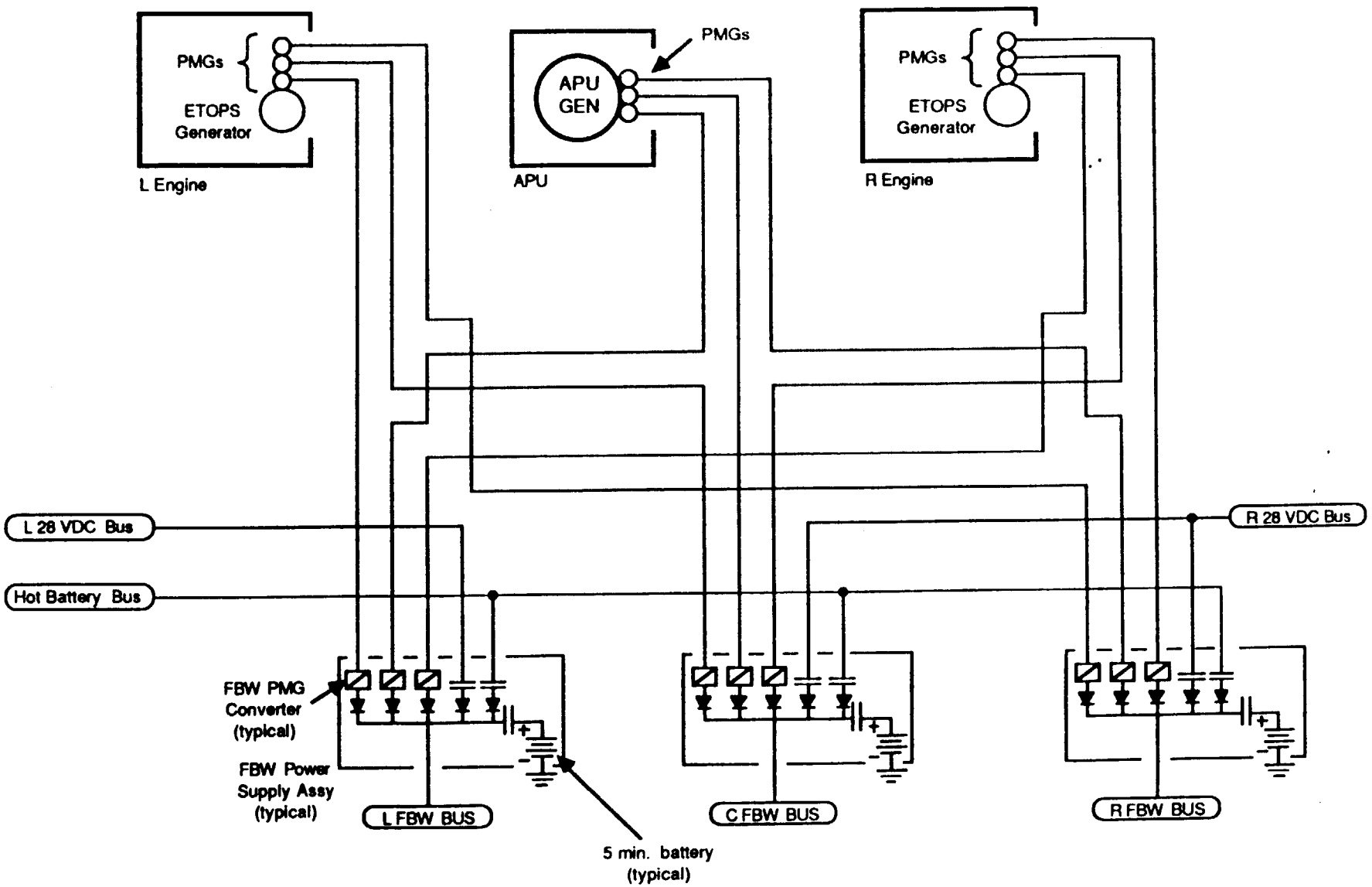
MAE 8 9 90 D4

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

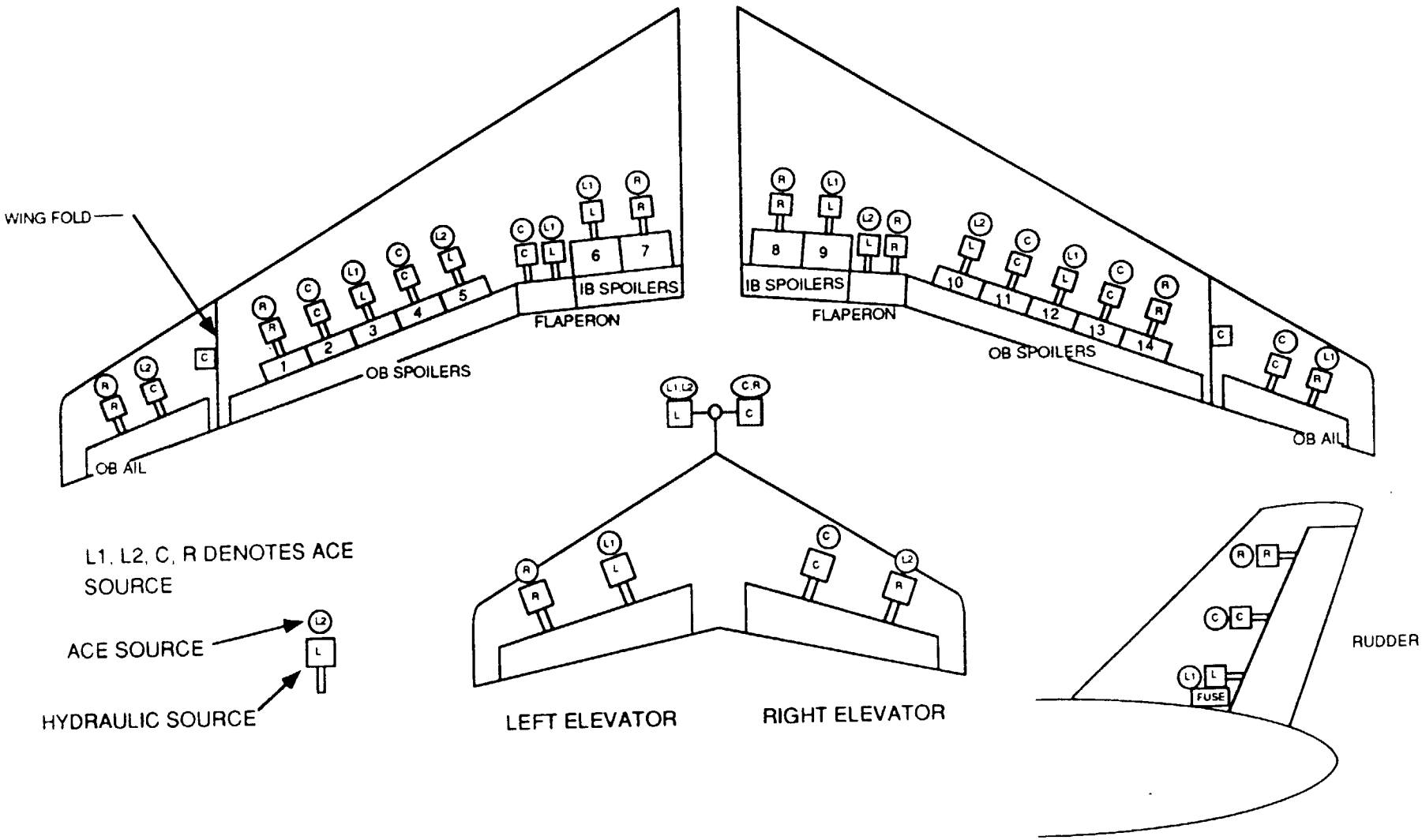


PRIMARY FLIGHT COMPUTER ARCHITECTURE

767-X ELECTRICAL POWER SYSTEM
FLIGHT CRITICAL DC



RNJ 7/6/90



767-X PRIMARY FLIGHT CONTROLS HYDRAULIC / ACE DISTRIBUTION

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

SAFETY

FEDERAL AVIATION ADMINISTRATION (FAA) REGULATIONS DEFINE THE BASIC SAFETY CRITERIA:

FAR 25.1309	**NO SINGLE FAILURE OR COMBINATION OF FAILURES WHICH ARE NOT SHOWN TO BE EXTREMELY IMPROBABLE SHALL PREVENT CONTINUED SAFE FLIGHT AND LANDING OF THE AIRPLANE**

EXTREMELY IMPROBABLE - PROBABILITY OF 1×10^{-9} OR LESS PER FLIGHT HOUR OR EVENT

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

SAFETY

FEDERAL AVIATION ADMINISTRATION (FAA) REGULATIONS DEFINE THE BASIC SAFETY CRITERIA:

FAR 25.1309	NO SINGLE FAILURE OR COMBINATION OF FAILURES WHICH ARE NOT SHOWN TO BE EXTREMELY IMPROBABLE SHALL PREVENT CONTINUED SAFE FLIGHT AND LANDING OF THE AIRPLANE

EXTREMELY IMPROBABLE - PROBABILITY OF 1×10^{-9} OR LESS PER FLIGHT HOUR OR EVENT

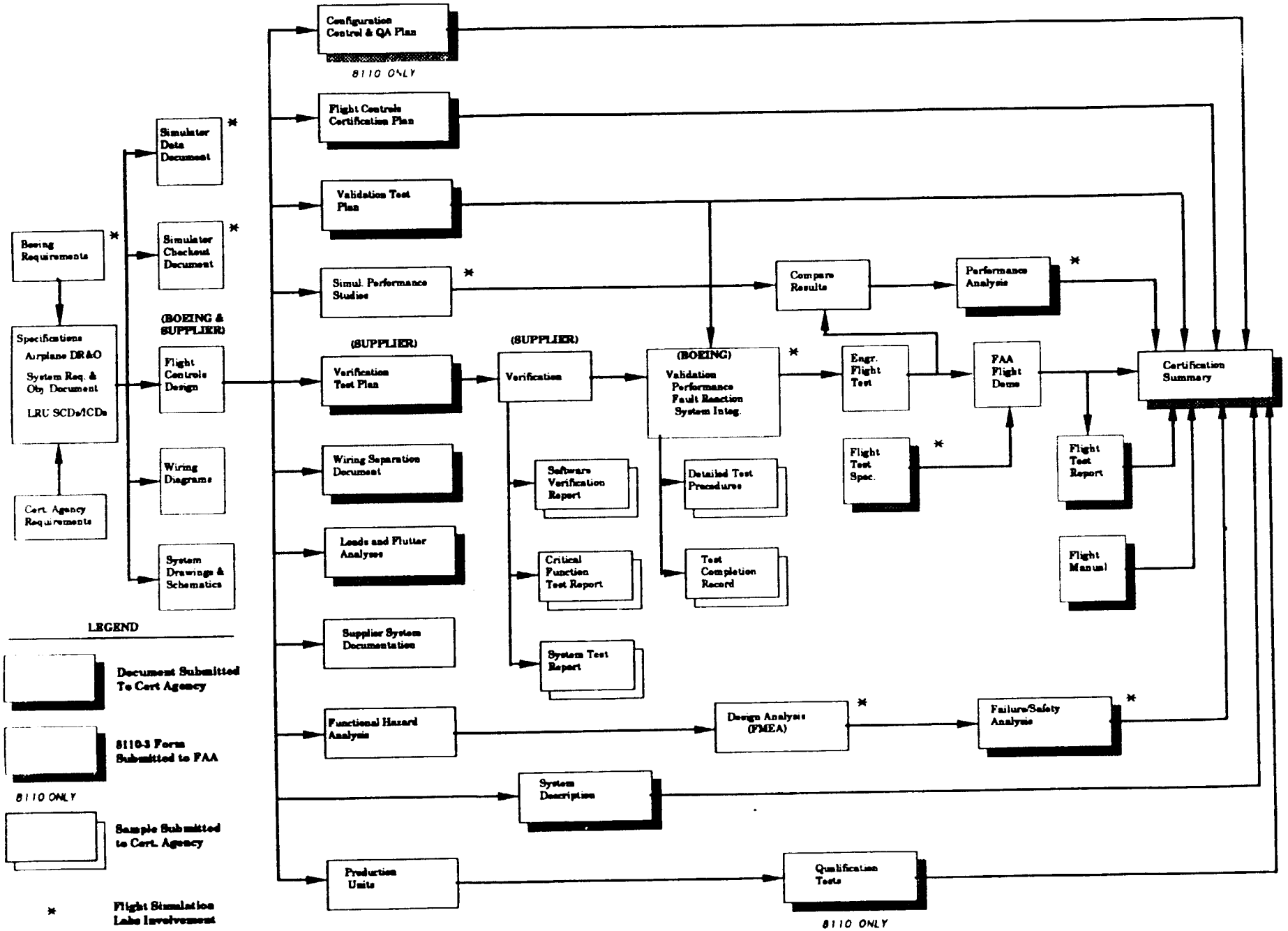


FIGURE 1.2-1 PRIMARY FLIGHT CONTROLS DEVELOPMENT OVERVIEW

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - REQUIREMENTS DEFINITION

TOP DOWN STRUCTURED PROCESS:

AIRPLANE LEVEL REQUIREMENTS	TOP LEVEL DESIGN REQUIREMENTS AND OBJECTIVES
SYSTEM REQUIREMENTS	CERTIFICATION REQUIREMENTS FUNCTIONAL REQUIREMENTS INTEGRITY REQUIREMENTS ARCHITECTURAL CONSIDERATIONS
SOFTWARE REQUIREMENTS	EXPANSION OF SYSTEM REQUIREMENTS TO A LEVEL WHICH CAN BE IMPLEMENTED IN A TARGET DIGITAL COMPUTER OR COMPUTERS

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - REQUIREMENTS DEFINITION

TOP DOWN STRUCTURED PROCESS:

AIRPLANE LEVEL REQUIREMENTS	TOP LEVEL DESIGN REQUIREMENTS AND OBJECTIVES
SYSTEM REQUIREMENTS	CERTIFICATION REQUIREMENTS FUNCTIONAL REQUIREMENTS INTEGRITY REQUIREMENTS ARCHITECTURAL CONSIDERATIONS
SOFTWARE REQUIREMENTS	EXPANSION OF SYSTEM REQUIREMENTS TO A LEVEL WHICH CAN BE IMPLEMENTED IN A TARGET DIGITAL COMPUTER OR COMPUTERS

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - DESIGN AND DEVELOPMENT

HARDWARE SELECTION	I/O REQUIREMENTS
	PROCESSING SPEED
	MEMORY SIZE
	ETC
PROGRAMMING LANGUAGE	INDUSTRY/COMPANY STANDARD
	SUPPORT SOFTWARE AVAILABILITY AND MATURITY
	LONG TERM MAINTENANCE
	ETC
CODE GENERATION	TYPICALLY AN INCREMENTAL BUILD PROCESS
TESTING	HARDWARE - QUALIFICATION TESTING - RTCA DO-160
	INCREMENTAL SOFTWARE LOADS - VENDOR AND AIRFRAME
	SYSTEMS INTEGRATION / IRON BIRD
	AIRPLANE - GROUND AND FLIGHT

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - VERIFICATION

GUIDELINE DOCUMENT RTCA DOCUMENT DO-178A

VERIFICATION PROCESSES ARE A FUNCTION OF SYSTEM CRITICALITY

CRITICAL SYSTEM	**A FORMAL PROCESS OF ASSURING THAT ALL SOFTWARE REQUIREMENTS HAVE BEEN IMPLEMENTED COMPLETELY AND EXCLUSIVELY**

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - VALIDATION

A PROCESS OF ASSURING THAT ALL SYSTEM REQUIREMENTS HAVE BEEN IMPLEMENTED CORRECTLY

- ANALYSES

SAFETY ANALYSIS	HAZARD ASSESSMENT AND FAILURE ANALYSIS TO ASSURE THAT REQUIREMENTS OF FAR 25.1309 ARE SATISFIED
PERFORMANCE ANALYSIS	ASSURANCE THAT SYSTEM PERFORMS INTENDED FUNCTION WITHIN ACCEPTABLE LIMITS UNDER ALL ALLOWABLE ENVIRONMENTAL AND TOLERANCE CONDITIONS

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - VALIDATION

A PROCESS OF ASSURING THAT ALL SYSTEM REQUIREMENTS HAVE BEEN IMPLEMENTED CORRECTLY

- ANALYSES

SAFETY ANALYSIS	HAZARD ASSESSMENT AND FAILURE ANALYSIS TO ASSURE THAT REQUIREMENTS OF FAR 25.1309 ARE SATISFIED
PERFORMANCE ANALYSIS	ASSURANCE THAT SYSTEM PERFORMS INTENDED FUNCTION WITHIN ACCEPTABLE LIMITS UNDER ALL ALLOWABLE ENVIRONMENTAL AND TOLERANCE CONDITIONS

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - CERTIFICATION

THE PROCESS OF DEMONSTRATING TO THE REGULATORY AUTHORITIES THAT ALL SAFETY AND PERFORMANCE REQUIREMENTS ARE SATISFIED

STARTS WITH A CERTIFICATION PLAN WHICH:

- IDENTIFIES REGULATIONS AND ACCEPTABLE MEANS OF COMPLIANCE METHODS
- DESCRIBES PROPOSED METHODS OF ESTABLISHING COMPLIANCE
- DESCRIBES THE METHODS AND PROCESSES TO BE USED TO ASSURE AN ORDERLY AND CONTROLLED DESIGN AND DEVELOPMENT PROCESS

FOLLOW ON SPECIALIST MEETINGS

PERFORMANCE AND INTEGRITY DEMONSTRATIONS

LIFE-CRITICAL DIGITAL FLIGHT CONTROL SYSTEMS

PROGRAM PHASES - CERTIFICATION (CONT)

CERTIFICATION SUMMARY

CONFIRMS COMPLETE IMPLEMENTATION OF THE PROCESSES IDENTIFIED IN THE CERTIFICATION PLAN

PROVIDES A MEANS FOR ESTABLISHING VERIFICATION AND VALIDATION COVERAGE

767-X PFCS Schedule