Fault Tolerance, Fault Diagnostics, and Prognostics in Flight Control Systems

Dave Bodden
Senior Fellow
Lockheed Martin Aeronautics

Background - Some LM Aeronautics Products

- F-35 Joint Strike Fighter
- C-27J Spartan
- C-5 Galaxy
- F-16 Fighting Falcon
- F-2 Defense Fighter
- P-3 Orion
- S-3 Viking
- T-50 Golden Eagle

F-117 Nighthawk

F-22 Raptor

C-130 Hercules

F-16 Fighting Falcon

C-5 Galaxy

F-35 Lightning II

U-2 Dragon Lady

F35 (JSF)

- The F35 Has Unique (and Extremely Demanding Requirements!
- Develop 3 Variants With a Common Airframe

X-35A Conventional (Air Force)

X-35C Carrier Suitable (Navy)

X-35B Short Takeoff/Vertical Landing Variant (Marines)

A Cautioner's Tale

I'm a little High-Risk and Patience is my name.
I'm really rather expert at causing pain.
I'm stealthy and deceptive and destruction is my game.
You'll know when I've been busy by the chaos, smoke, and flame.

This flying business is certainly a feat.
The pilots like the challenge, they say it's hard to beat.
The engineers are striving to mitigate the risk.
By now they know my talents and the pace is pretty brisk.

I'm really an admirer of the engineering mind,
But your thoroughness and detail are a stultifying grind.
I much prefer to function in a random sort of way
And haven't yet decided what I'll do today!

In wires, pumps, and filters, actuators and in code;
In sensors, chips, connectors, I oft' make my abode.
In complicated systems and even simple switches;
I have so many faces – it's hard to find the glitches.

A Cautioner's Tale

I quite enjoy the solitude of resting in my lair.
In general, I take no umbrage when my home takes to the air.
But when you turn the heat up and shake me from my bed,
You'd better be observant, be careful how you tread.

If e'er you see me working, I think you'll be impressed;
You'll understand the value of exhaustive test.
Approach the task with vigor, intelligence and zest,
For if you hope to find me you mustn't ever rest.

A Cautioner's Tale

Should your system-level testing turn out a trifle weak,
Then rest assured the outcome would probably be bleak.
Be perceptive in your planning, let omissions be remote….

Or I'll fool your fancy logic and calmly slit your throat!!

Author Unknown

Flight Critical Systems

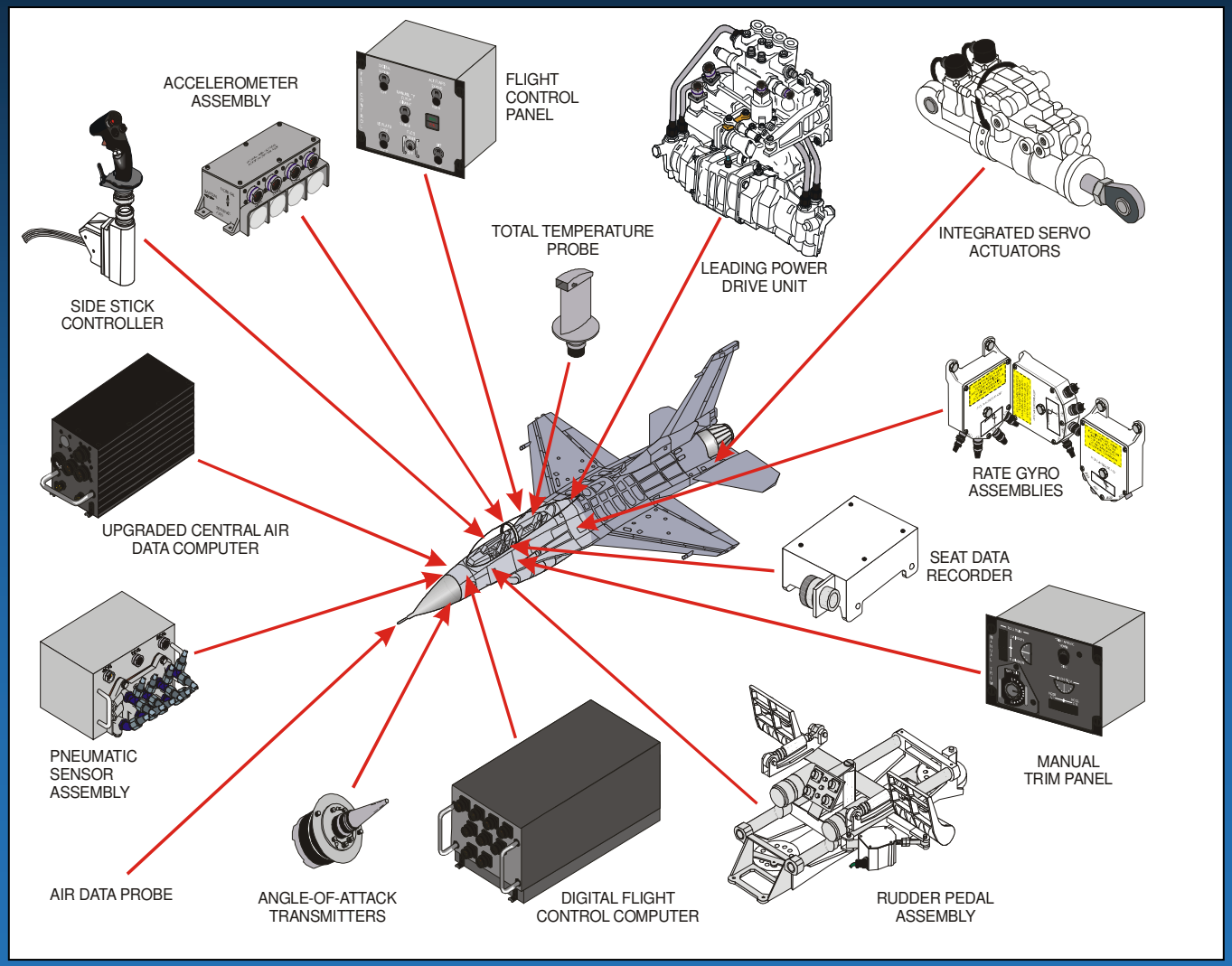
- A class of system specifically designed to limit the consequence of hazards related to:
  - ***Probability-Of-Loss of Control (PLOC)***
    - **Allocated from aircraft loss rate**
  - ***Survivability***
    - **Gunshots**
    - **Catastrophic Failures**
  - ***Aircraft Performance***
    - **Stability**
    - **Handling qualities**
  - ***Crew Safety***
    - **Structural interactions**
    - **Load limitations**
    - **Human limitations**

Fault Tolerance in Flight Critical Systems

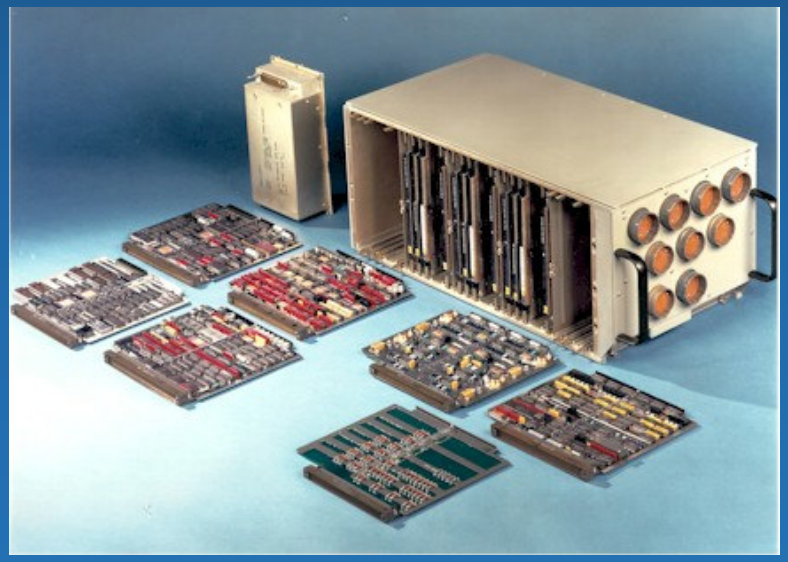
- **Redundant System Design**
  - ***Physical***
  - ***Functional***
  - ***Temporal***
  - ***Inductive***
- **Integrity Management**
  - ***Built in Test (BIT)***
  - ***System Integrity Monitors***
- **Robust Control Law Design**
  - ***Feedback Control Design***
  - ***Control Reconfiguration***

Physical System Redundancy

- **Achieved by allowing identical Processes to be Performed on Multiple Identical Physical Devices – Weight and Cost Negatives.**

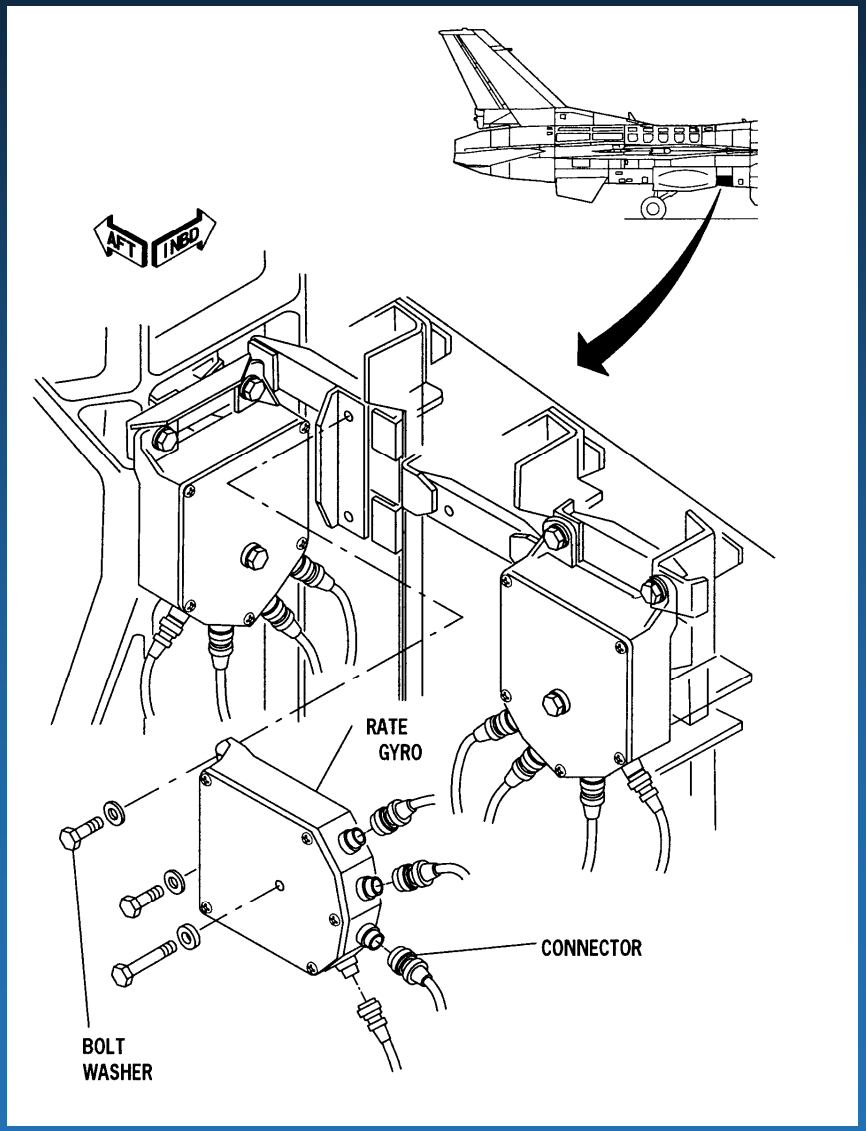


Digital Flight Control Computer



- **QUAD-REDUNDANT ELECTRONICS**
- **CONSOLIDATES FLCC, ECA, & FCP ELECTRONICS OF ANALOG SYSTEM**
- **SINGLE LRU FOR EASY INSTALLATION AND REMOVAL**
- **MULTIPLE CONNECTORS FOR CHANNEL SEPARATION & REDUNDANCY**
- **PERFORMS INTERNAL AND EXTERNAL SYSTEM BUILT-IN-TEST FUNCTION**
- **Mil-1750 Processor**
  ~ .7 Mips
- **48K Words Memory**
- **Single Mil-1553 RT**
- Weight: **62.5 Lbs**

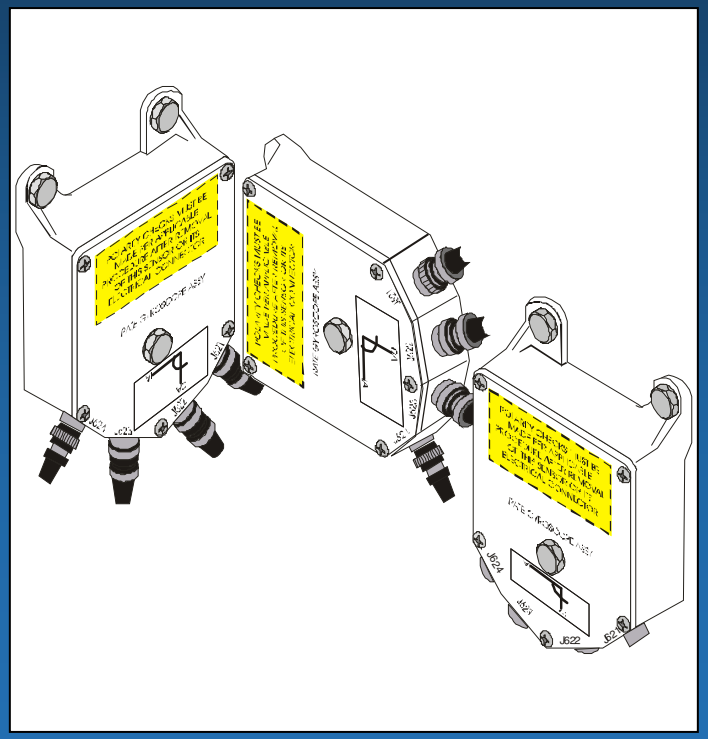
Rate Gyro Assemblies



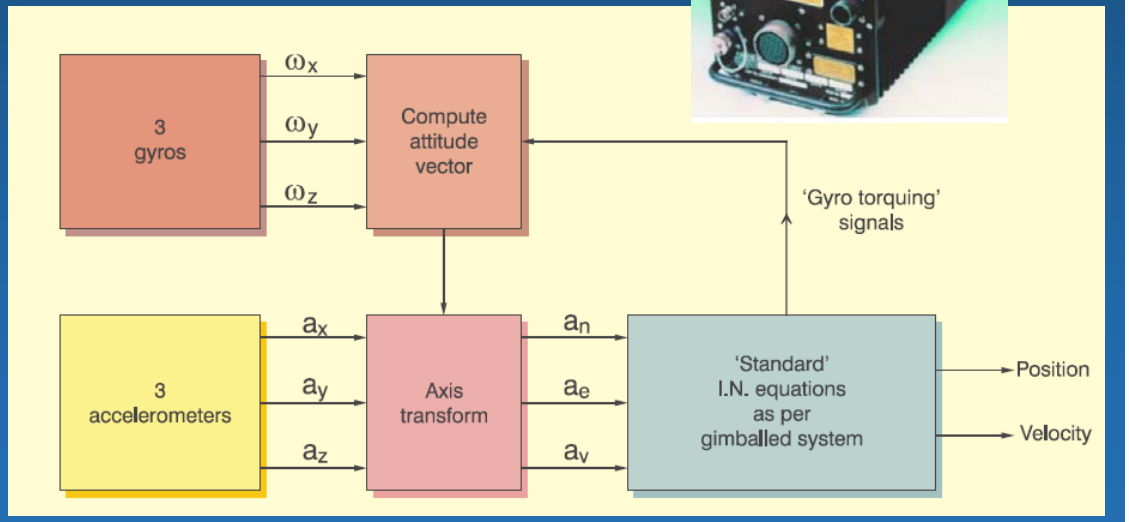
- SEPARATE RATE GYRO ASSEMBLIES UTILIZED FOR PITCH, ROLL, AND YAW AXES
- QUAD-REDUNDANT
  - *EACH ASSEMBLY CONTAINS FOUR IDENTICAL RATE GYROS*
- EACH GYRO OUTPUTS A SIGNAL CORRESPONDING TO AIRCRAFT BODY RATES DEPENDING ON INSTALLATION ORIENTATION
- EACH GYRO OUTPUTS A MONITOR SIGNAL AS A FUNCTION OF SPIN MOTOR SPEED
- EACH GYRO ACCEPTS A TORQUE SIGNAL FOR SELF-TEST CAPABILITY

Functional Redundancy

- **Achieved by Allowing Identical processes to be Performed on Different Hardware**
  - ***Rate Gyros, INS, EGI***
  - ***Dissimilar Hardware***



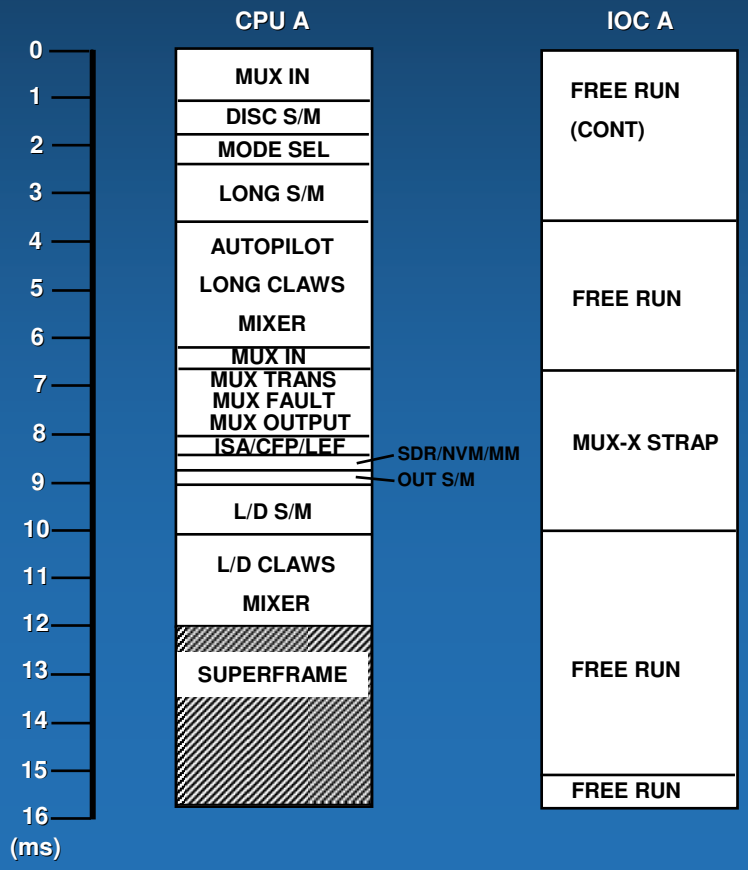
Typical Flight Control Grade Rate Gyros



Strapdown Inertial Navigation System

Temporal Redundancy

- **Achieved by Allowing Identical Processes to be performed at Different Points in Time**
  - ***Commonly Used to Check Communications Data Integrity, Communication Paths, and Insuring CPU Sanity***
  - ***Watchdog Timers, Heartbeat Monitors***

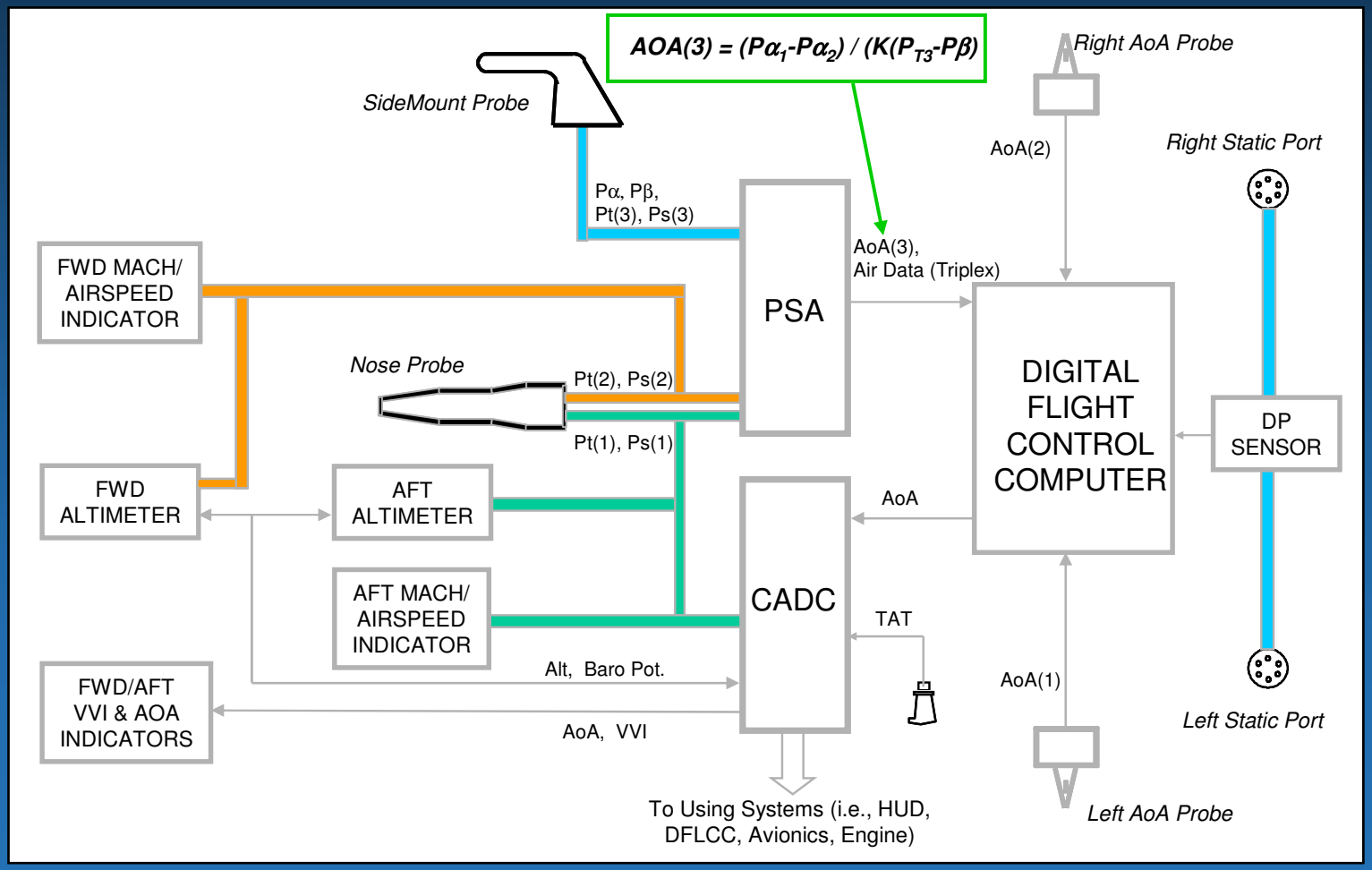


F16 Flight Control System Operates Asynchronously

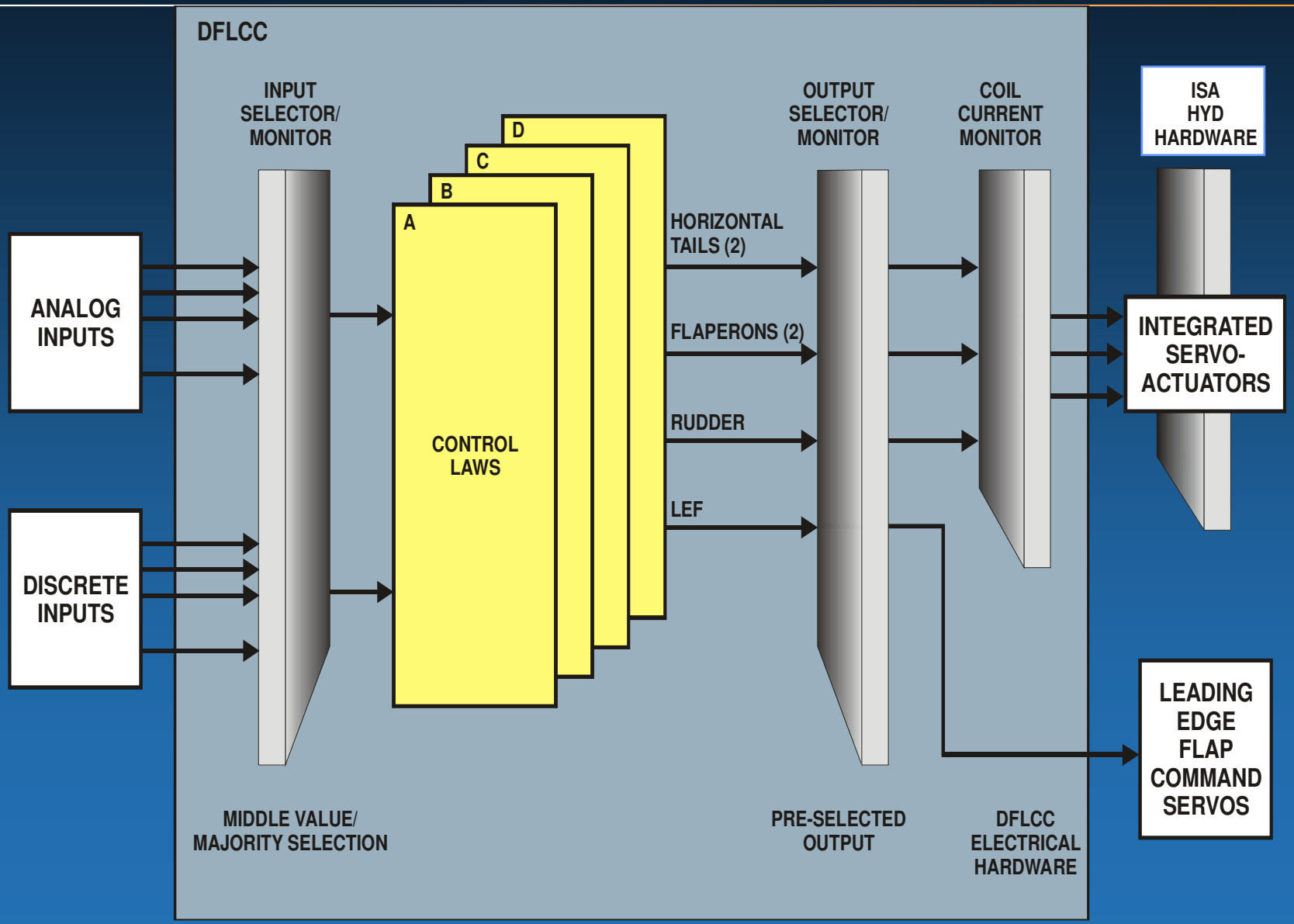
- ***CPU and IOC For a Given Channel Run Independently***
- ***Channels are Not Frame Synchronized***

Inductive Redundancy

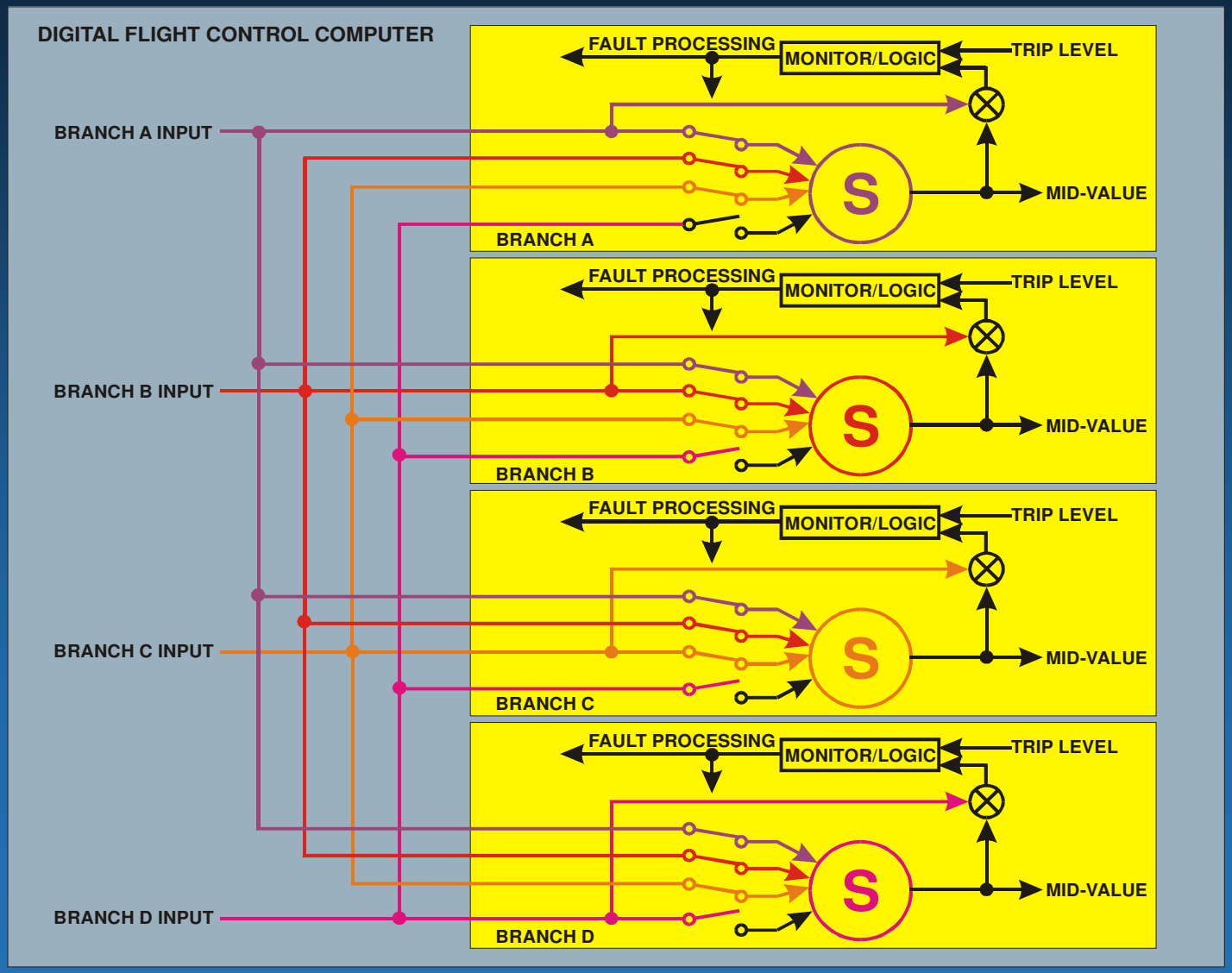
- **Achieved by Cross-Correlating Different but Related Processes with One Another**
  - ***Commonly Used in Estimation Techniques***



Redundancy Implementation – F16



Input Selector Monitor



Mid - Value Select

Consider the Following Values for AOA

A = 10.3°
B = 10.1°
C = 10.2°

Average Value = 10.2°
Mid-Value = 10.2°

After a Failure in Branch B, Consider the Following Values for AOA

A = 10.3°
B = 56.0°
C = 10.2°

Average Value = 25.5°
Mid-Value = 10.3°

A Mid – Value Select Minimizes Errors Associated with Failures Until the Device is Declared Failed (Exceeds Persistence Count)

Diagnostics and Integrity Management

System Integrity Management Applies The Idea of "Verticality of Testing"

- Equipment Qualification (ATPs)
- Pre-Flight BIT
- In-Flight Monitoring
- Post-Flight BIT
- Maintenance BIT

Tolerances and Coverages Are Most Stringent

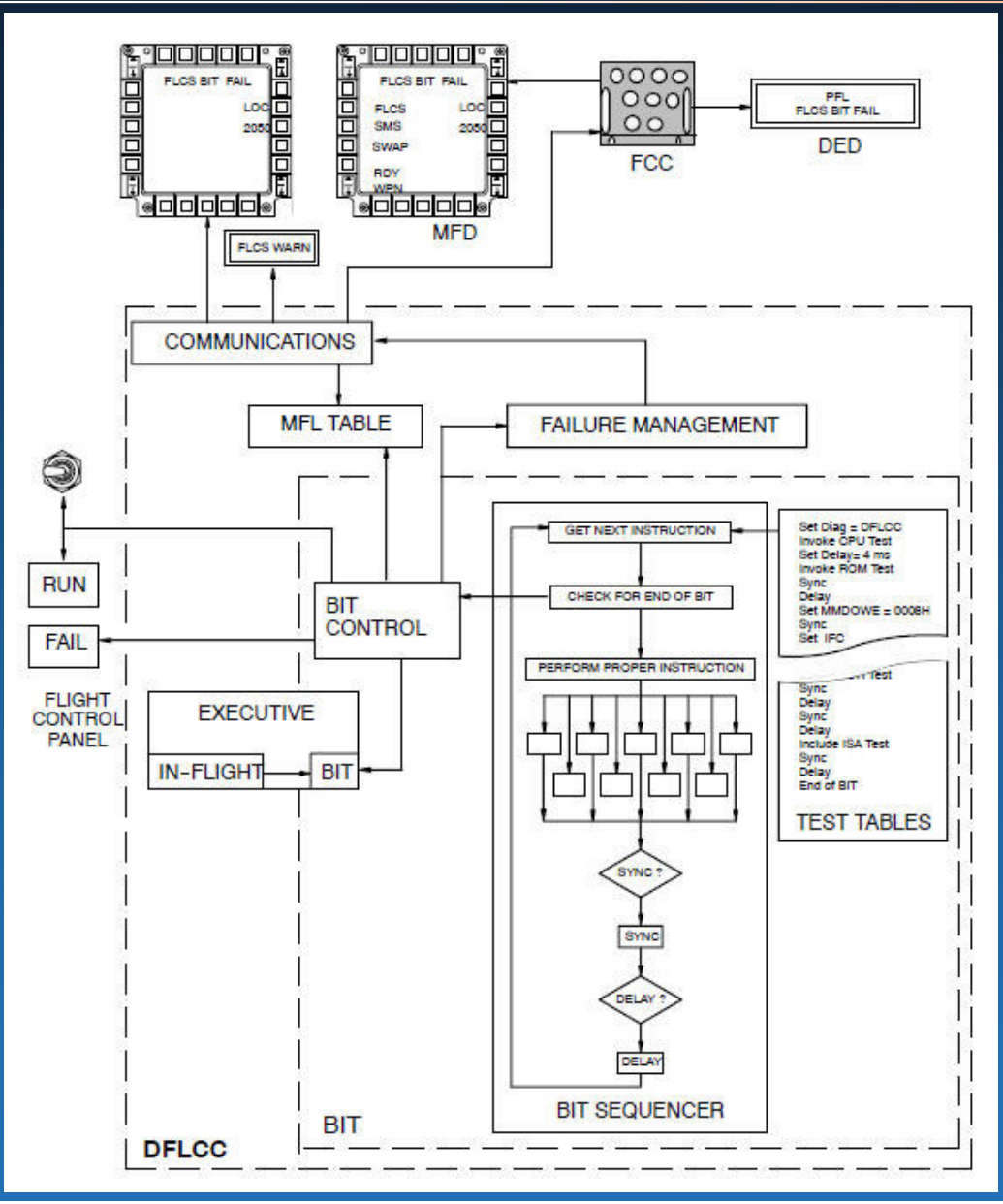
Widest Tolerance, Lowest Coverage

Tolerances and Coverages Are Most Stringent

The Elimination of Latent Failures Is The Object of all Ground Test Functions

Each Succeeding Level of Test Limits The Exposure of The System To Hazards

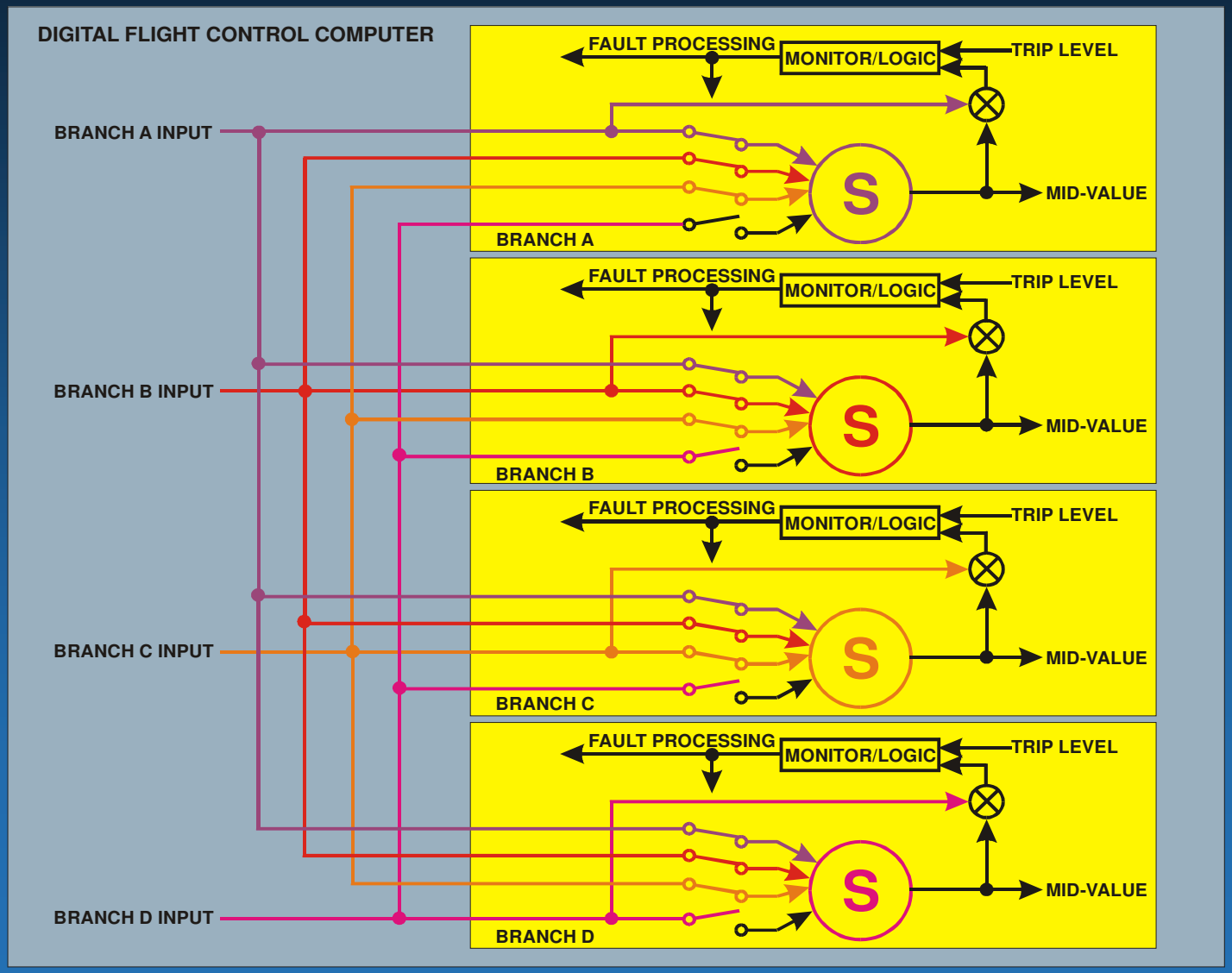
Typical Pre-Flight BIT



Typical BIT Checks

- CPU
- ROM
- RAM
- IOC File
- IOC Data Transmit
- MUX
- Reference Voltage
- Analog Addressing
- Analog Input
- Watch Dog Timer
- Discrete I/O
- Failure Logic
- AOA to CADC
- Coil Current Monitor
- Sensor
- NVM
- SDR
- MFT Flyup Disable
- CADC
- LEF
- ISA

Input Selector Monitor



Typical Input Monitor Trip Levels

FPSTK = 5 lbs	7 Frames
FRSTK = 3 lbs	7 Frames
FRUD = 15 lbs	7 Frames
NACL = .9g	7 Frames
LACL = .225g	7 Frames

AOA = - With the gear handle down and in-flight, Threshold = 6º
- Else threshold equals the Max Value of 6º, (–0.1333*QCSEL+48.67)

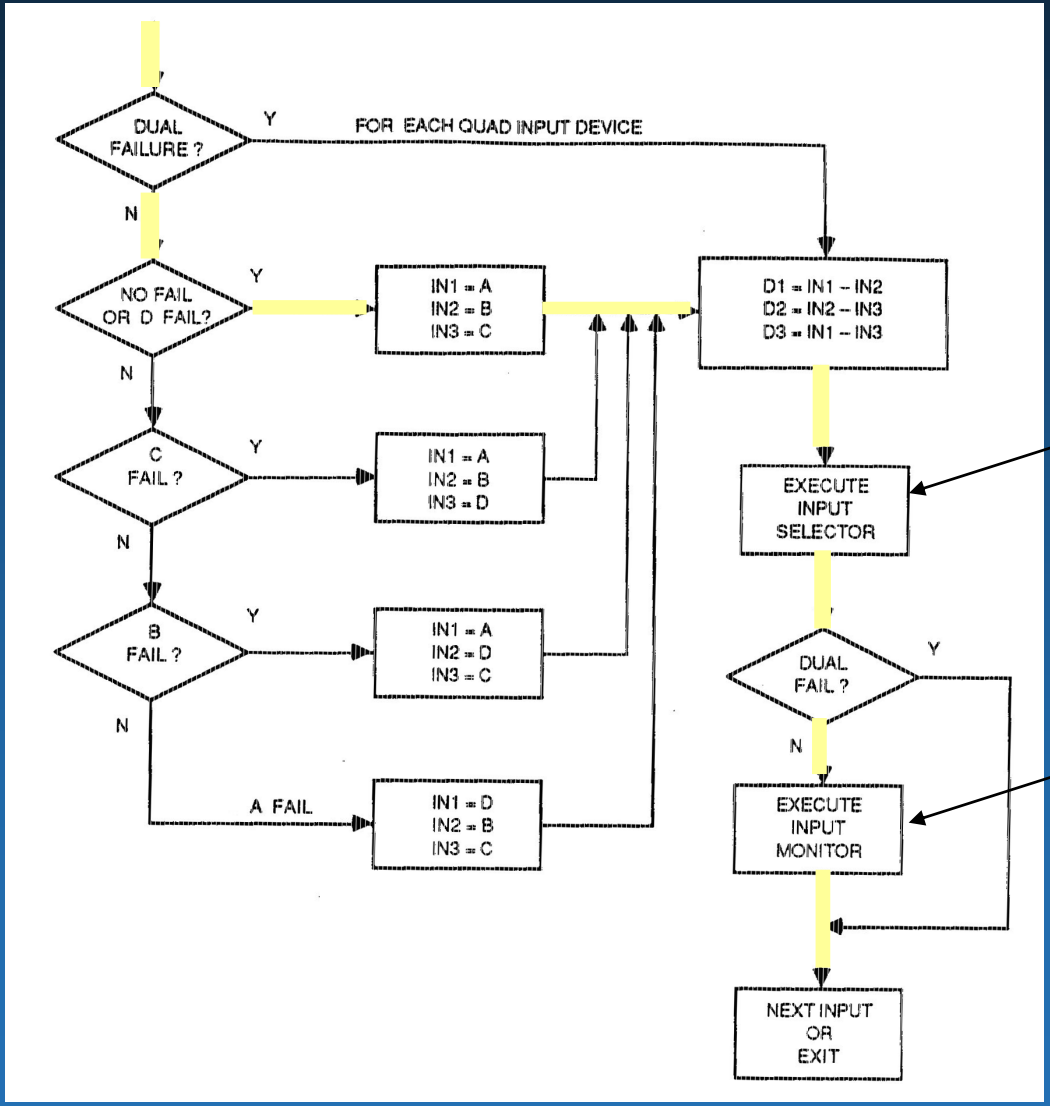
= Threshold increases above 6º when Qc < 300KCAS

Example: 170KCAS = 100psf

-0.1333 x 100psf = -13.33

-13.3 + 48.67 = 35.37º

Input Monitor Flow Diagram for Quad Devices



Mid Value Select

Fault Identification

Fault Identification for Quad Devices

|D1| > TL	N	N	N	Y	Y	Y	N	N	Y	Y	Y
|D2| > TL	N	N	Y	N	Y	Y	Y	Y	N	N	Y
|D3| > TL	N	Y	N	N	N	N	Y	Y	Y	Y	Y
PC = LIM 1	-	-	-	-	N	Y	N	Y	N	Y	-
ACTION	1	2	2	2	3	4	3	5	3	6	2

ACTIONS

1. IF NO FAILS
   - THEN IF |D - SEL| > TL
     - THEN IF PC = LIM 1
       - THEN FAIL INPUT D
       - ELSE INCREMENT PC AND TC
     - ELSE IF PC > 0
       - THEN DECREMENT PC
       - ELSE NO ACTION
   - ELSE IF PC > 0
     - THEN DECREMENT PC
     - ELSE NO ACTION
2. NO ACTION
3. INCREMENT PC AND TC
4. SET PC = 0
   - IF B FAILED
     - THEN FAIL INPUT D
     - ELSE FAIL INPUT B
5. SET PC = 0
   - IF C FAILED
     - THEN FAIL INPUT D
     - ELSE FAIL INPUT C
6. SET PC = 0
   - IF A FAILED
     - THEN FAIL INPUT D
     - ELSE FAIL INPUT A

Assume no Prior Failures With the Following Values for Pitch Rate and TL=6°/s

A = 10.5	A = 10.5	A = 10.5
B = 16.5	B = 16.6	B = 17.6
C = 11.5	C = 11.5	C = 11.5
D = 11.3	D = 11.3	D = 11.3
SEL= 11.5	SEL= 11.5	SEL= 11.5
D1 = -6	D1 = -6.1	D1 = -7.1
D2 = 5	D2 = 5.1	D2 = 6.1
D3 = -1	D3 = -1	D3 = -1

Start Persistence Count

Take No Action, TL Exceeded for Only One Channel

If No Prior Failures, Check to See if D is Within Tolerance

Robust Control Algorithms

A Bad Day at the Office

Basic SISO Feedback Control Algorithms Provide Fault Tolerance

A Bad Day at the Office - Continued

- *Control Reconfiguration Buys you Better Handling Qualities with Failures*
- *Adaptive Control Allows for Better Control Reconfiguration with Failures Undetectable by System Monitors, BIT, etc.*

A New Concept in Inductive Redundancy

Synthetic Redundancy via Prognostics

Synthetic Redundancy via Prognostics

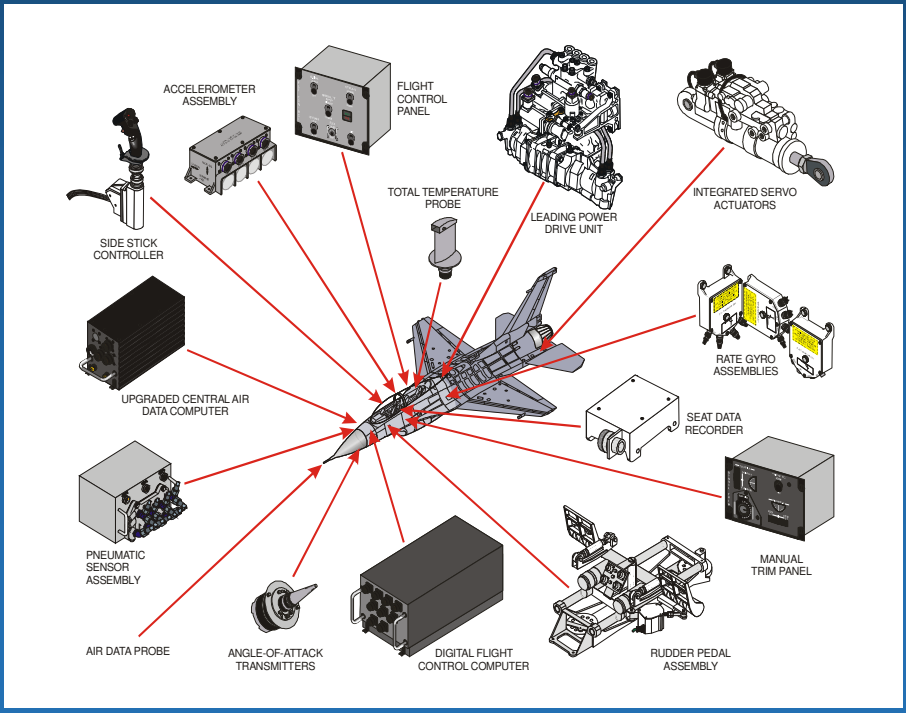
- **Prognostics Refers to the Future State of Reliability of a Component, Device, Subsysem, etc.**

- **The Current State-of-the-Art for Prognostics and Health Management (PHM) is centered on Condition Based Maintenance (CBM); i.e. performing Maintenance or Replacing Components as Required Rather than Scheduled.**

- "PHM as a Design Variable in Air Vehicle Conceptual Design", Bodden, D.S., et al., AIAA Journal of Aircraft, Vol 43, Number 4, Pages 1053-1058
- "Seeded Failure Testing and Analysis of an Electro-Mechanical Actuator", Bodden, D.S., and Clements, N.S., Proceedings of the IEEE Aerospace Conference, March 2007, Big Sky Montana
- "Seeded Fault Testing and In-situ Analysis of Critical Electronic Components in EMA Power Circuitry", Baybutt, M., Bodden, D.S., et.al., Proceedings of the IEEE Aerospace Conference, March 2008, Big Sky Montana.

Hypothesis 1

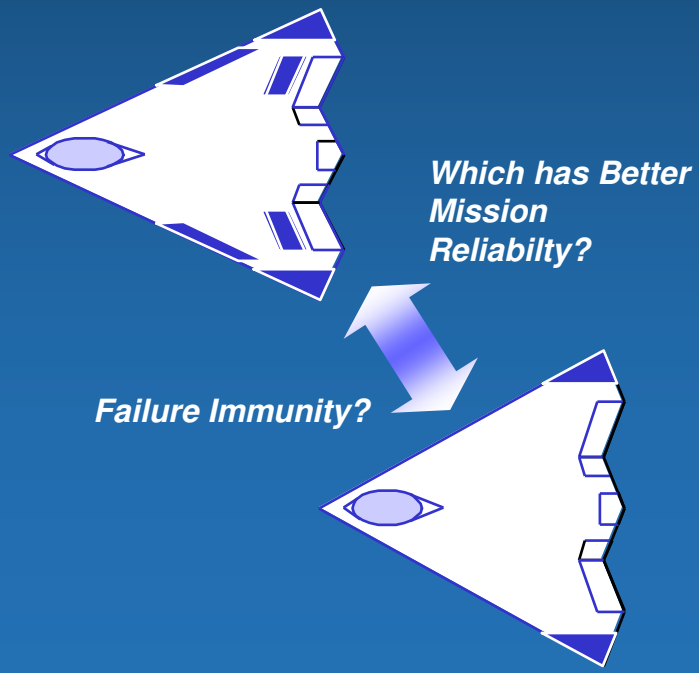
Accurate and Correct Implementation of Prognostics Technology Should Result in an Operational Reliability close to 1 for a Particular System, Sub-system, or Component



- *Realistic?*
- *Cost of Prognostics?*
- *Mechanical Systems?*
- *Electrical Systems?*
- *Eliminate Physical Redundancy?*

Hypothesis 2

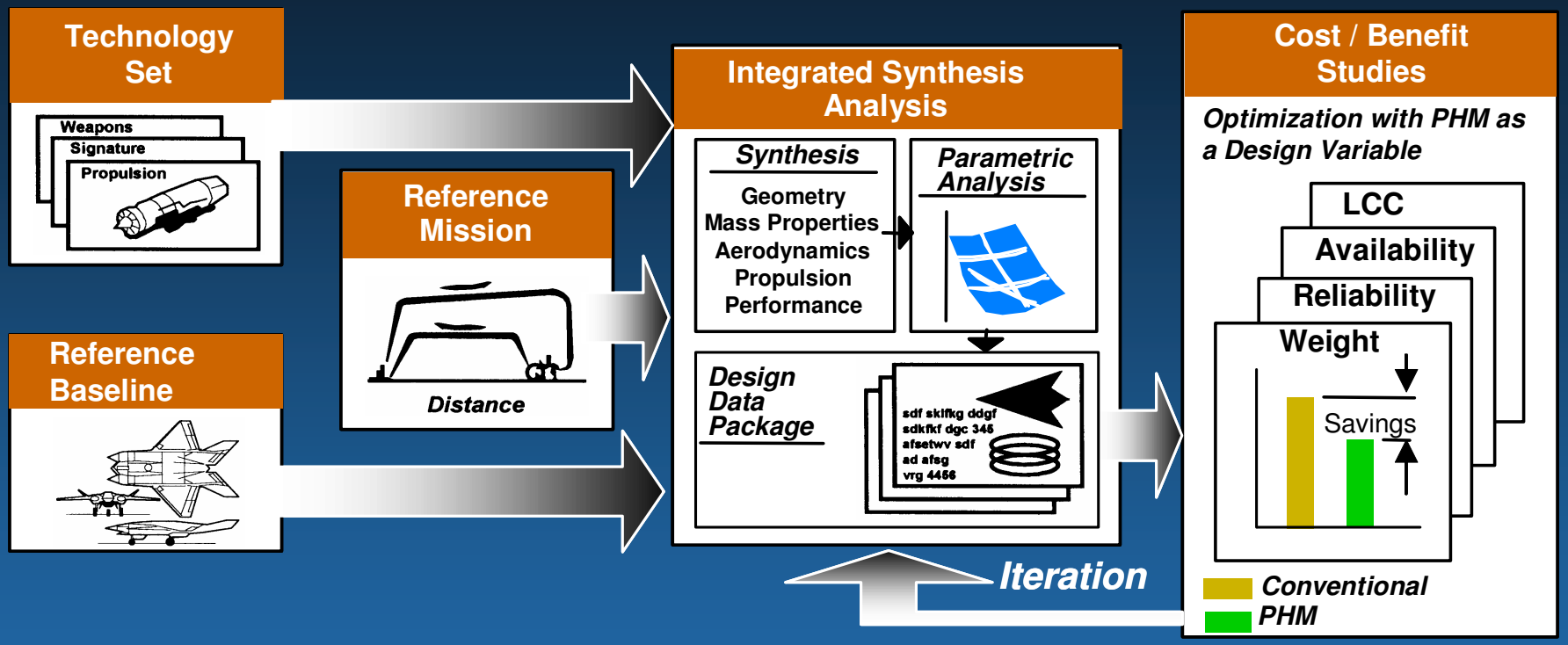
Optimization of the Air Vehicle Configuration for Reliability Facilitates An Optimal System/Subsystem Design



- ***Objective***

Optimize Number of Control Surfaces and Actuator Redundancy with Prognostics as a Design Variable

Air Vehicle Conceptual Design Process



- *Optimized for Performance*
- *"Modified" for Stability & Control, etc.*
- *Reliability in Subsystems as Required Through Redundancy and Reliable Components*

Optimize Primary Control Physical Redundancy Parameters
- ***Number Control Surfaces***
- ***Actuator Redundancy***

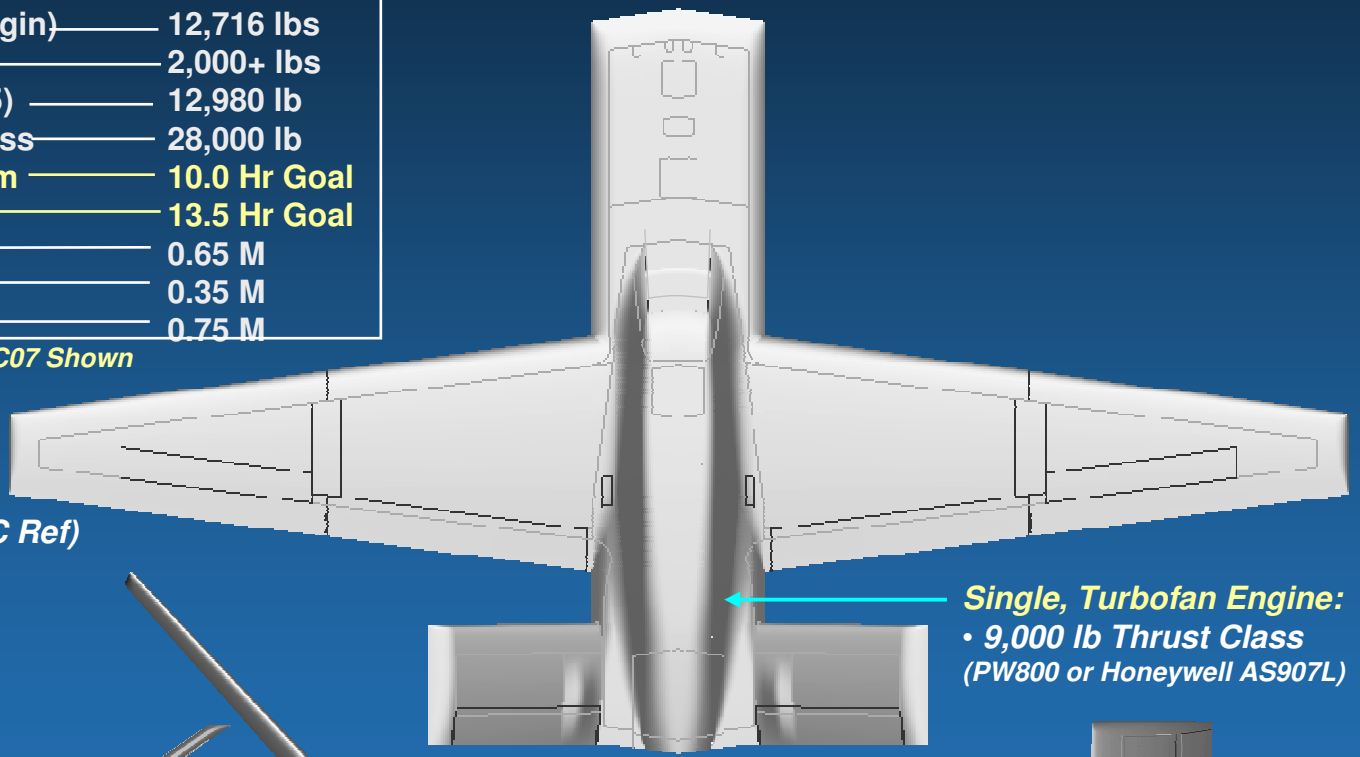
Sea Based Endurance (SBE) UAV Selected for Optimization Studies

Specifications	
Wing Span	66.56 Ft
Wing Area	560 Sq. Ft
Overall Length	37.00 Ft
Empty Weight (w/ 6% margin)	12,716 lbs
Internal Payload Weight	2,000+ lbs
Internal Fuel Weight (JP-5)	12,980 lb
Takeoff Gross Weight Class	28,000 lb
Time-On-Station @ 600 nm	10.0 Hr Goal
Total Mission Time	13.5 Hr Goal
Cruise Speed	0.65 M
Loiter Speed	0.35 M
Max Speed	0.75 M

Configuration SBE-C07 Shown

Carrier Suitable:

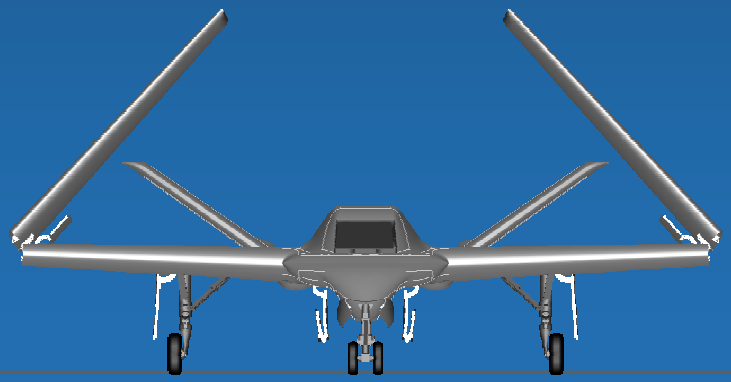
- *Catapult Launch*
- *Arrested Recovery*
- *1.02 Spot Factor (F/A-18C Ref)*

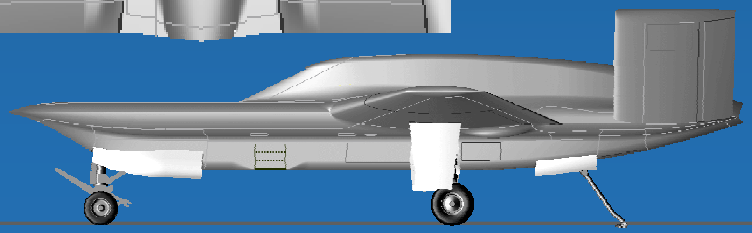


Single, Turbofan Engine:

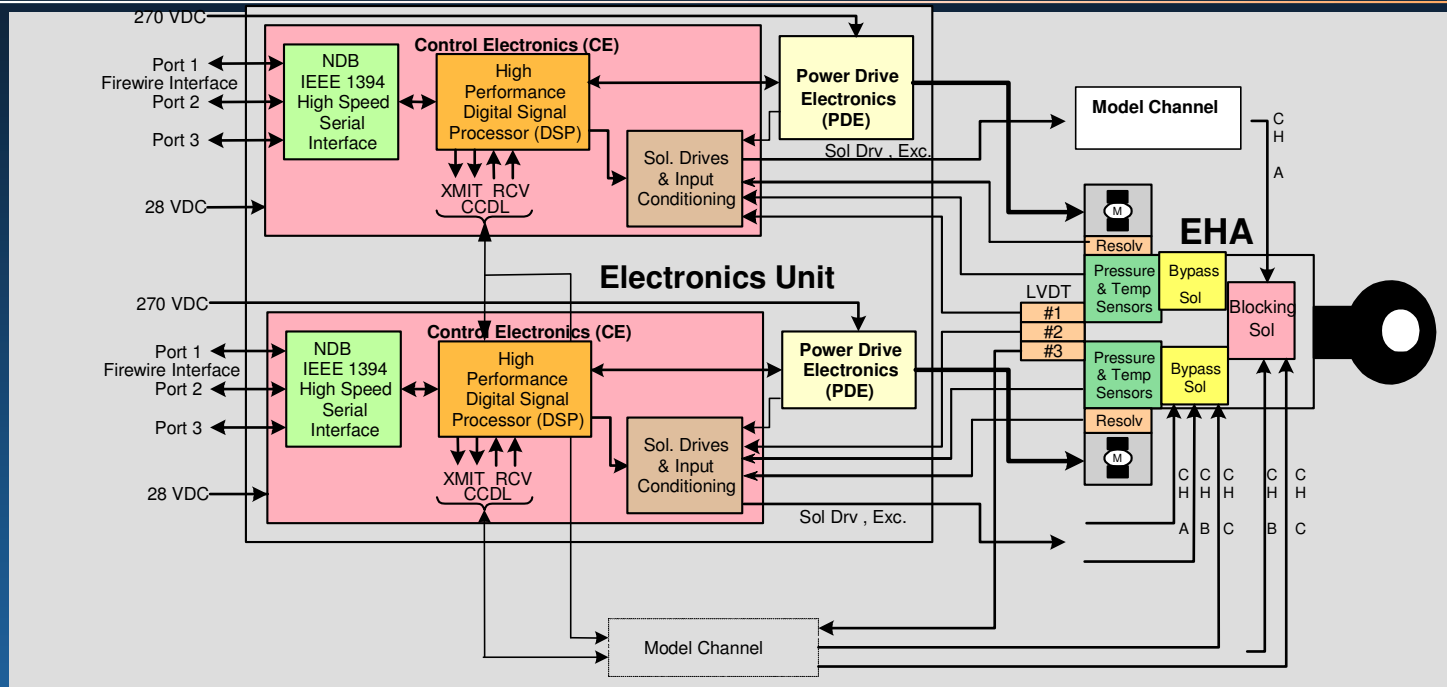
- *9,000 lb Thrust Class*

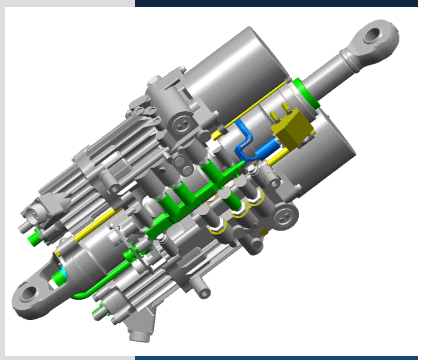
(PW800 or Honeywell AS907L)

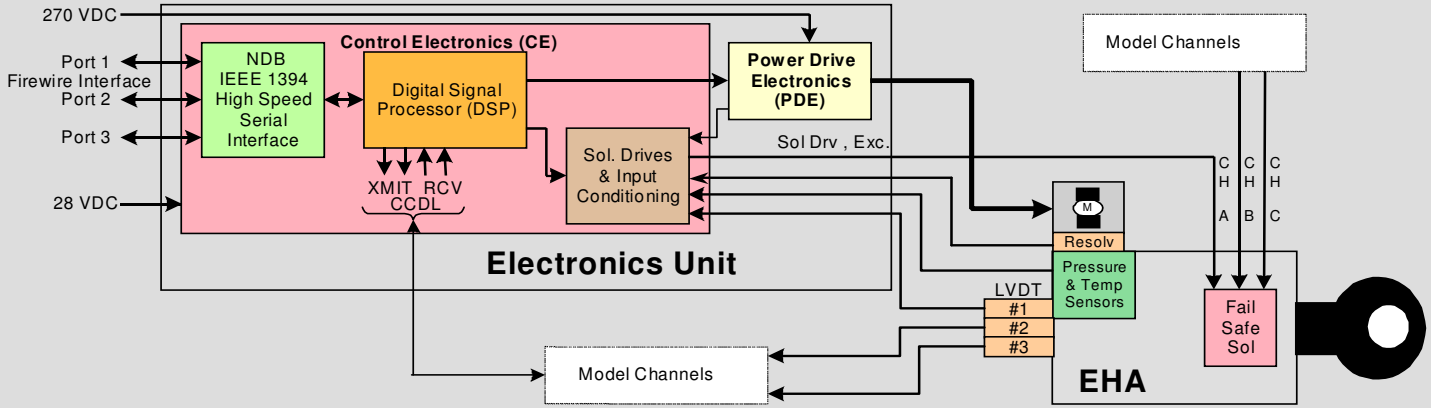


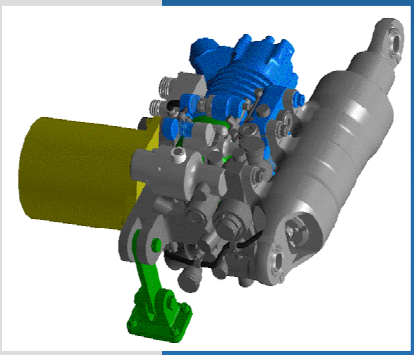


Electro Hydrostatic Actuators









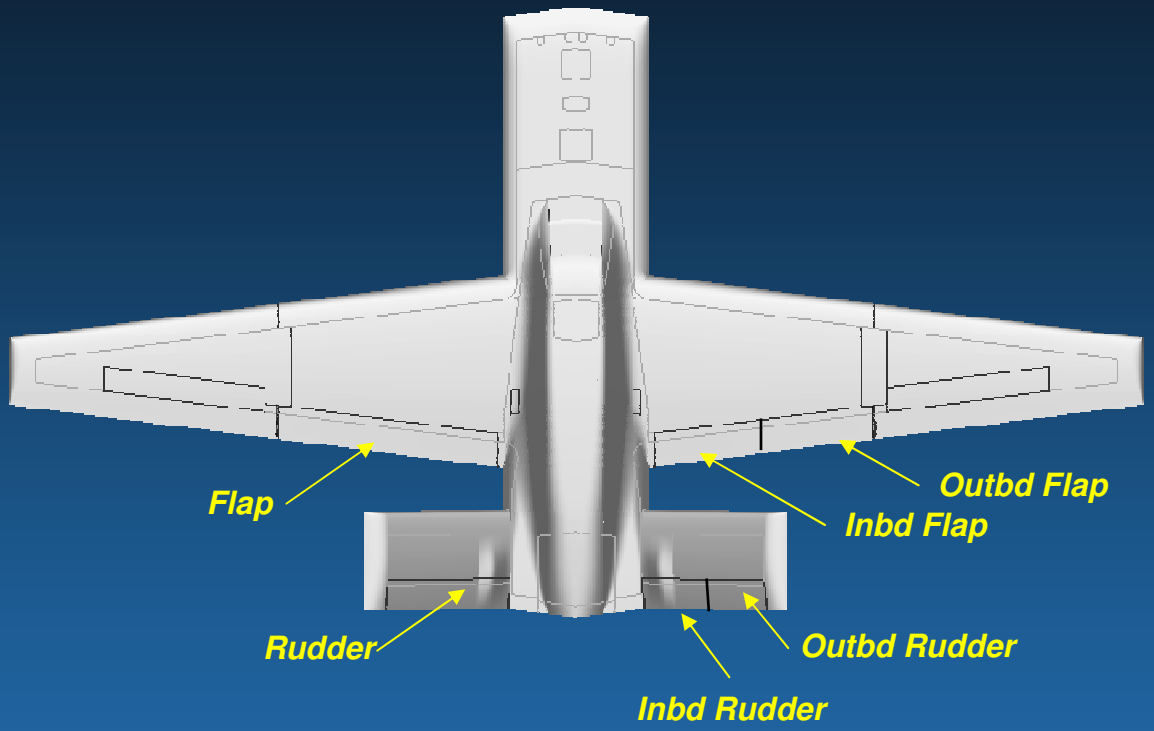
Optimization Space

j Airframe Configuration

1. Nominal*
2. Split Flaps
3. Split Rudders
4. Split Flaps & Rudders

k Actuator Configuration

1. Simplex Actuators/ Simplex Electronics
2. Duplex Actuators
3. Simplex Flap/ Duplex Rudder
4. Simplex/ Duplex Electronics



m PHM Configuration

1. no PHM
2. With EHA PHM 85%
3. With EHA PHM 60%
4. With EHA PHM 35%
5. No PHM with TCI

*Nominal Configuration
- No Split Surfaces
- k=2, m=1, n=1

n Failure State

1. no Failures
2. Left Rudder
3. Left Flap
4. Inbd Flap
5. Outbd Flap
6. Inbd Rudder
7. Outbd Rudder
8. Left Rudder 2nd Fail
9. Left Flap 2nd Fail
10. Left Flap/Right Rudder
11. Inbd Rudder/Inbd Flap
12. Inbd Rudder/Outbd Flap
13. Outbd Rudder/Inbd Flap
14. Outbd Rudder/Outbd Flap
15. Left Inbd Rudder/Left Outbd Rudder
16. Left Inbd Flap/Left Outbd Flap
17. Right Inbd Rudder/Left Flap

Reliability Criteria

Several Criteria Evaluated as Reliability Constraints for Optimizing the Air Vehicle Configuration

- √ **Failure Immunity**
  - *Addresses Consequences of Failure of any Component*
  - *Based on Fault Tree Analysis and Adjusted Supplier MTBF Data*
- √ **Probability of Loss of Aircraft (PLOA) or Mission Reliability (In the Context of this Application)**
  - *Overall Roll Up of Reliability Allocations*
  - *Estimate of Number of Aircraft Lost per xx Flt Hrs or Missions*
  - *Based on Fault Tree Analysis and Adjusted Supplier MTBF Data*
- √ **Mission Availability**
  - *Measure of Percentage of Time Aircraft Would be Available*
  - *Based on Adjusted Supplier MTBF Data and Time To Repair an LRU*

Optimization Problem

Optimize the Air Vehicle Design to Minimize the Air Vehicle Weight and Life Cycle Cost, Subject to the Following Constraints:

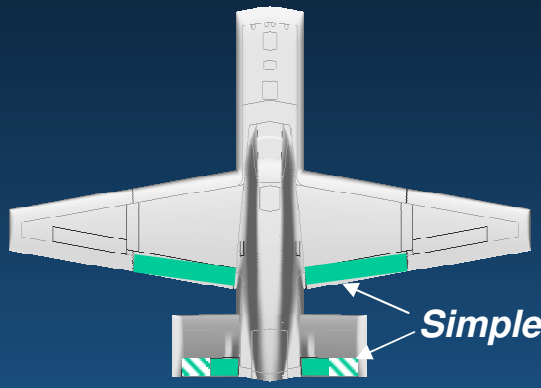
- **Carrier Landing Dispersion**
  - ***-60<x<20***
  - ***-10≤y≤10***

- **Mission Reliability (Flt Control Actuator PLOA Allocation)**
  - **≤ .13 Crashes per 10000 Flights**
  - **≤ .43 Crashes per 10000 Flights (13.5 Hour Flight)**

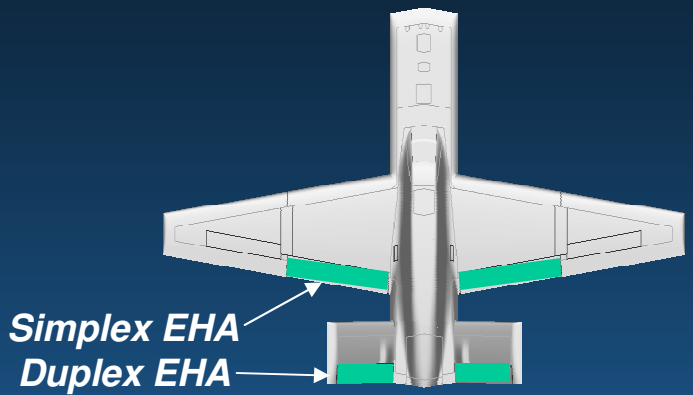
Optimization Parameters are:
j, k, m

- **Mission Availability**
  - **> 99%**

Optimization Results



Configuration j=3, k=4



Configuration j=1, k=3

CASE	Mission Reliability Constraint (Failures/10000 Missions)		PHM Effectivity Required	Δ Weight* (lbs)	Δ LCC* ($M)	Optimal Configuration		
	0.13	0.43				j	k	m
1. No PHM^	X		-	-45	-11.7	3	4	1
2. No PHM - TCI^	X		-	-45	21.6	3	4	5
3. EHA PHM^	X		35%	-45	-11.8	3	4	4
4. EHA/EU PHM	X		60%	-101	-35.7	1	3	3
5. No PHM^		X	-	-45	-11.7	3	4	1
6. No PHM - TCI		X	-	-101	-14.6	1	3	5
7. EHA PHM		X	35%	-101	-33.1	1	3	4
8. EHA/EU PHM		X	35%	-101	-32.7	1	3	4

** Relative to Baseline Configuration* *^ Did not Meet Mission Availability Constraint*