Making Embedded Digital Electronic Control Systems Satisfactorily Reliable

Defining "satisfactorily reliable"

(i) usable in the design of aircraft meant to carry many civilians

(ii) here "reliable" doesn't mean "no failures", it means "fail safe"

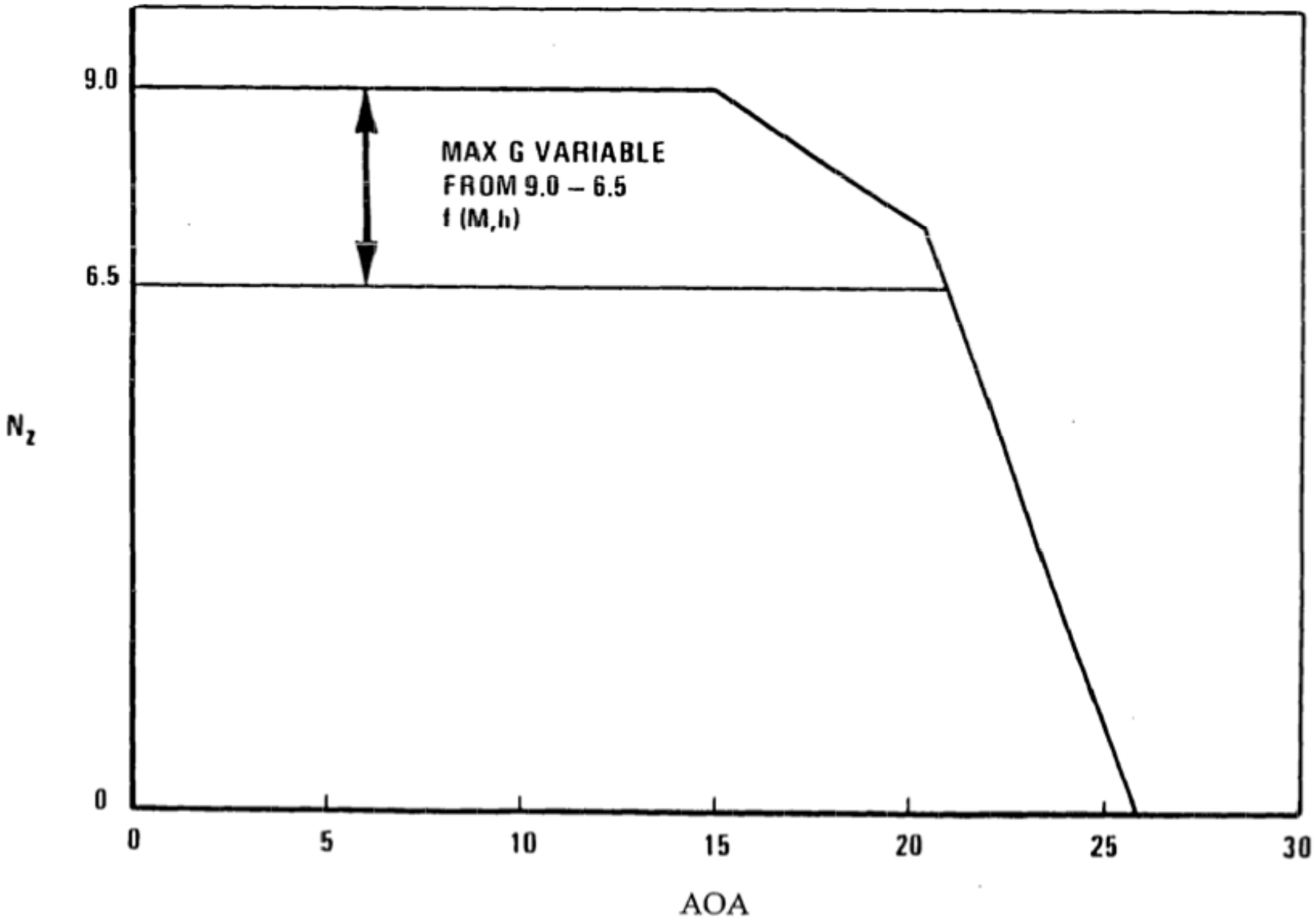
(iii) as dependable in flight operations, regarding safety of flight, as major load-carrying structural components

Isn't that their status now?

(i) used in redundant flight path control and and stability augmentation systems (SAS's)

(ii) used in load-limiting and other aspects of Vehicle Management Systems in military aircraft

(iii) not used to ensure safety of commercial travelers (nor in most military applications) where elimination of adverse consequences is beyond capabilities of human controllers (eg. "flutter", aeroelastic instability)


9.0
6.5
0
N_z
MAX G VARIABLE
FROM 9.0 – 6.5
f (M,h)
0
5
10
15
20
25
30
AOA

CLASSIFICATION	COMPONENTS	REDUNDANCY LEVELS
Flight Critical	• Cockpit Controls • PFCS Software • Control Surface actuators • Flight Instruments	Quad/Triplex
Flight Phase Essential	• AFCS Software • AFCS Sensors • MFDs	Triplex/Dual
Non-Critical	• Autopilot • Flight Director Displays	Dual/Single

Comparison of Systems to Provide Safety *

Aircraft	Mechanical Back-Up of FBW/FBO
Concord	All three axes
F-16	None
Airbus Transports	Rudder (yaw & roll) & trimmable stabilizer (pitch)

* i.e. eliminate adverse consequences of failures

Why is this important for vertical lift aircraft?

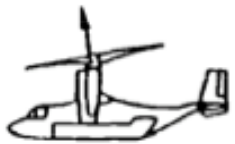
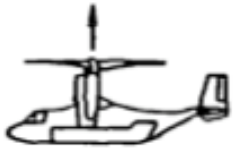
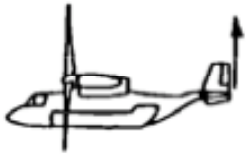
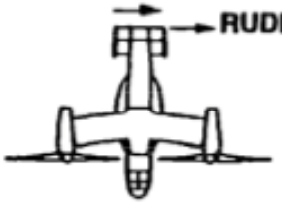
(i) Vertical flight demands lighter weight

(ii) Blade aeroelastic stability is now ensured by "balance" weights with magnified penalties (acceleration fields at blade tips of around 600 "g's")

(iii) Capability for unprepared terminal, close to ground obstruction operations, etc. call for new sensors/piloting aids

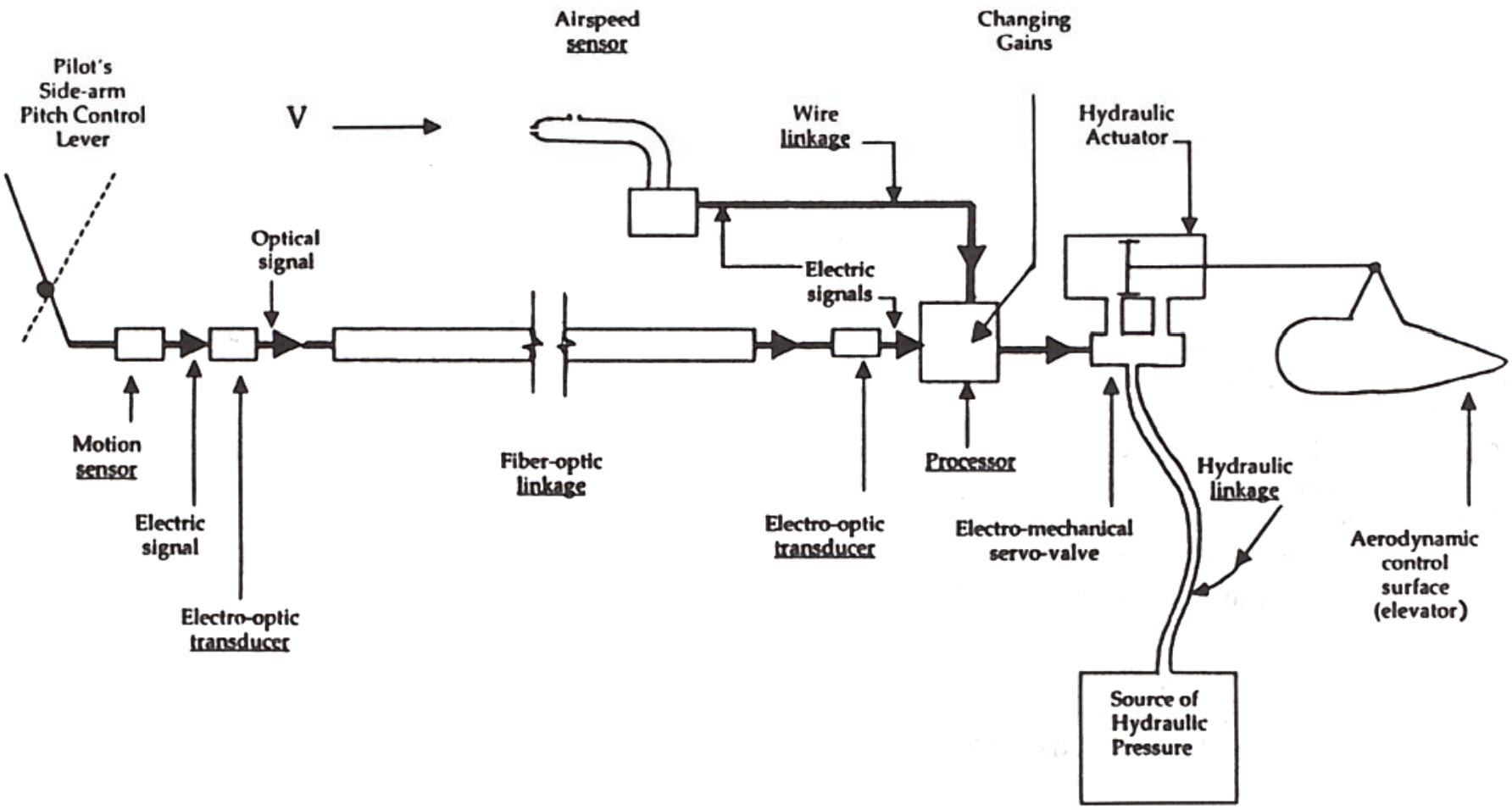
(iv) There are benefits to automated entry to autorotations, automated "flares", etc.

(v) Flight path control transitions with "morphing" (Tilt rotor, Tail-wing, Jet lift, VTOL's)

CONTROL AXIS			
PITCH	**ROLL**	**THRUST**	**YAW**
VTOL MODE			
LONGITUDINAL CYCLIC	DIFFERENTIAL COLLECTIVE PITCH AND LATERAL CYCLIC	THROTTLE/COLLECTIVE	DIFFERENTIAL LONGITUDINAL CYCLIC
			*LEFT ROTOR* *RIGHT ROTOR* 
AIRPLANE MODE			
ELEVATOR	FLAPERONS	THROTTLE / COLLECTIVE	RUDDER
			

Flight Control System Elements Subject to Failure

- Motion Sensor, electrical output
- Electro-Optic Transducer
- Electrical or Optical Linkages
- Airspeed Sensor
- Electro-mechanical servo-valve
- Hydraulic/Electric/Pneumatic Actuator
- Mechanical Linkage
- Aerodynamic surface


Airspeed sensor
Changing Gains
Pilot's Side-arm Pitch Control Lever
V
Wire linkage
Hydraulic Actuator
Optical signal
Electric signals
Motion sensor
Electric signal
Electro-optic transducer
Fiber-optic linkage
Electro-optic transducer
Processor
Electro-mechanical servo-valve
Hydraulic linkage
Aerodynamic control surface (elevator)
Source of Hydraulic Pressure

Is "Fail Safety" Just a matter of Hardware?

(i) Single computer control of multi tasks, multi-systems

(ii) Growth in the required number of "lines" in software "codes"

* typical current software line counts:

F22	1.7 million
F35	5.7 million
787	6.5 million

(iii) Cost of ensuring reliability; eg. 50% of new auto costs (per IBM)

Means to Increase Safety (i.e., be "fail-safe")

(i) Redundant architecture (reduces reliability)

(ii) "Voting" among redundant elements, and appropriate shut-down

(iii) Accepting the penalties of applying different designs for the same function in one system

(iv) Formal methods to verify control software