System Safety

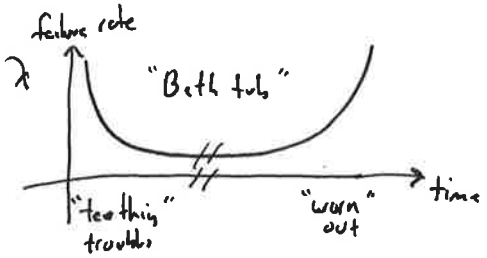
- Mean Time Between Failures (MTBF) $= T_m$ — on-condition: replace when failed

  failures per hour $= \lambda = \frac{1}{T_m}$

  $P(t) = 1 - e^{-\lambda t} \approx \lambda t - \frac{(\lambda t)^2}{2!} + \frac{(\lambda t)^3}{3!} + \cdots \approx \lambda t$ when λ is small

- MIL-STD-781

$$\lambda = \underbrace{\lambda_Q}_{\text{Quality}} \left(\underbrace{K_1 \lambda_T}_{\text{temp}} + \underbrace{K_2 \lambda_E}_{\text{environment}} \right) \underbrace{\lambda_L}_{\text{Maturity}}$$



- Hazard Level requirements

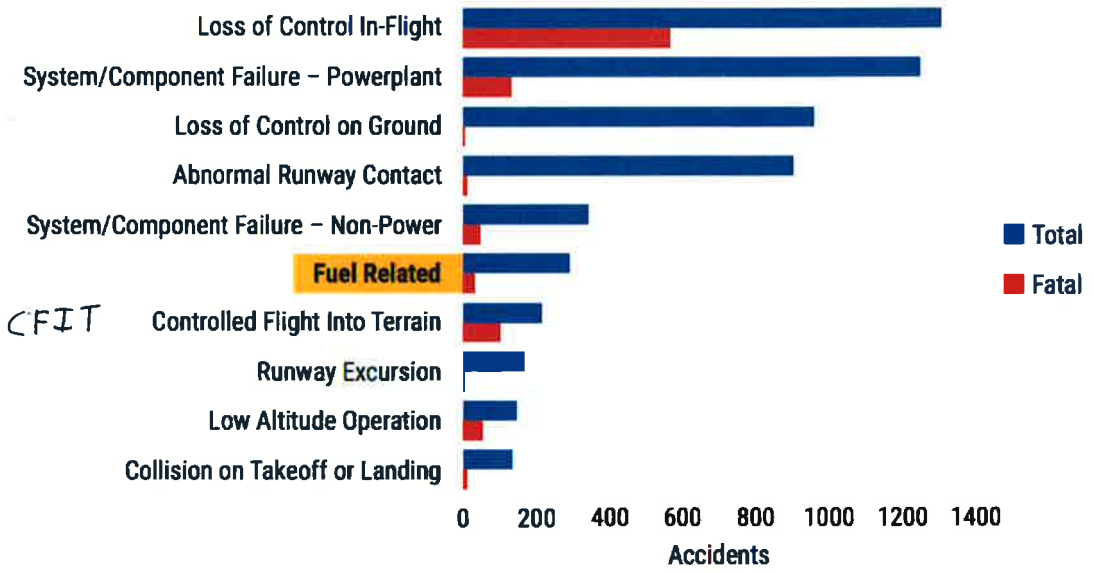
			Ofln?
Minor:	$\lambda < 1 \times 10^{-3}$ 1/hr, simplex	Some discomfort	Several times per airplane
Major:	$\lambda < 1 \times 10^{-5}$ 1/hr, duplex redundancy	Distress + Injuries	≈ 1 per airplane
Hazardous:	$\lambda < 1 \times 10^{-7}$ 1/hr, 3x redundancy	Fatal Injury	Few in type
Catastrophic:	$\lambda < 1 \times 10^{-9}$ 1/hr, 4x redundancy	Multiple Fatal	Never in type

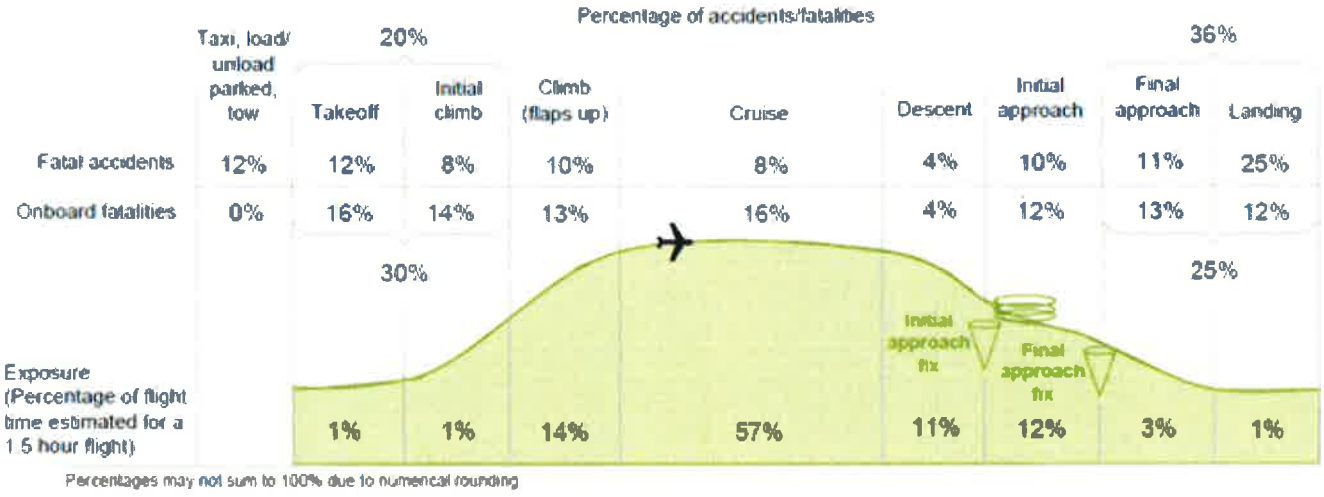
EFFECT ON AIRCRAFT AND OCCUPANTS	Normal	Nuisance	Operating limitations; emergency procedures	Significant reduction in safety margins: difficult for crew to cope with adverse conditions; passenger injuries	Large reduction in safety margins; crew extended because of workload or environmental conditions; serious injury or death of small number of occupants	Multiple deaths; usually with loss of aircraft	EFFECT ON AIRCRAFT AND OCCUPANTS
FAR 25 PROBABILITY		PROBABLE		IMPROBABLE		EXTREMELY IMPROBABLE	FAR 25 PROBABILITY
JAR 25/CS PROBABILITY	FREQUENT		REASONABLY FREQUENT	REMOTE	EXTREMELY REMOTE	EXTREMELY IMPROBABL E	JAR 25/CS PROBABILITY
FAILURE RATE (per flight hour)		10^{-3}	10^{-5}	10^{-7}	10^{-9}		
CATEGORY OF EFFECT		MINOR		MAJOR	HAZARDOUS	CATASTROPHIC	CATEGORY OF EFFECT

Figure 4.7 Probabilities and severity of effects

Source: CAS

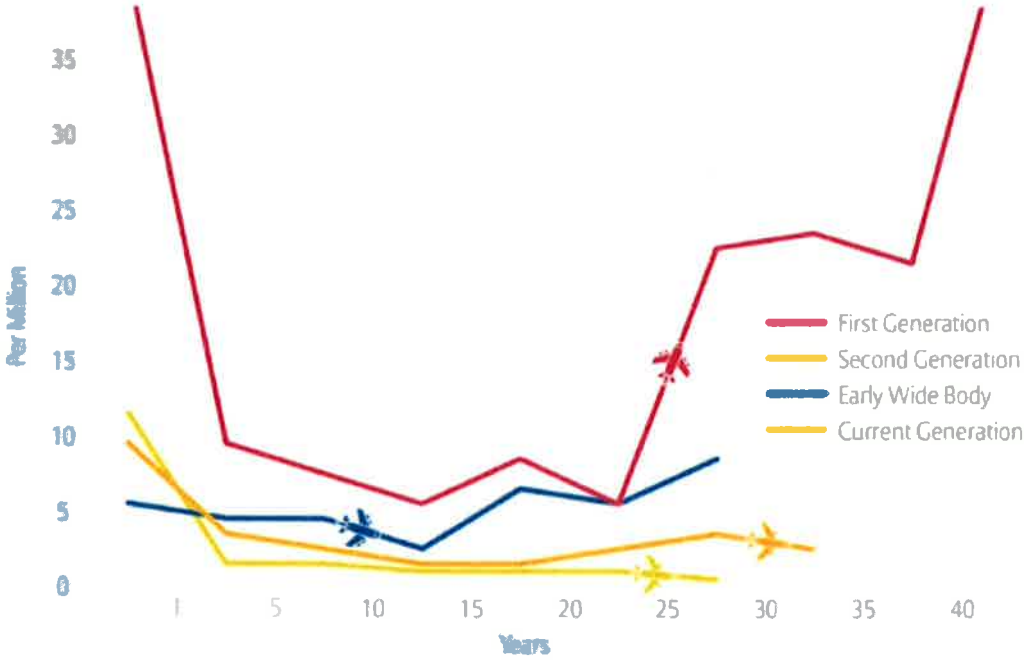
Figure 1. Top Ten General Aviation Accident Occurrence Categories, 2011–2015





Statistical Summary of Commercial Jet Airplane Accidents, 1959 - 2008, Boeing

Accident Rates Jet Aircraft by Generation per 1 Million departures



Graphic: Allianz Global Corporate & Specialty

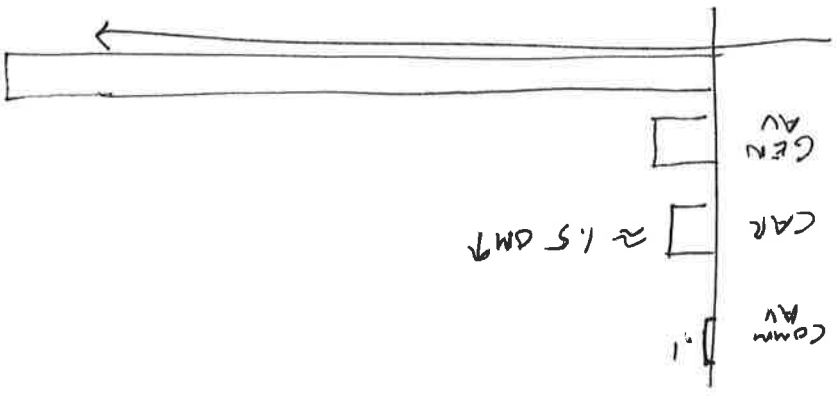
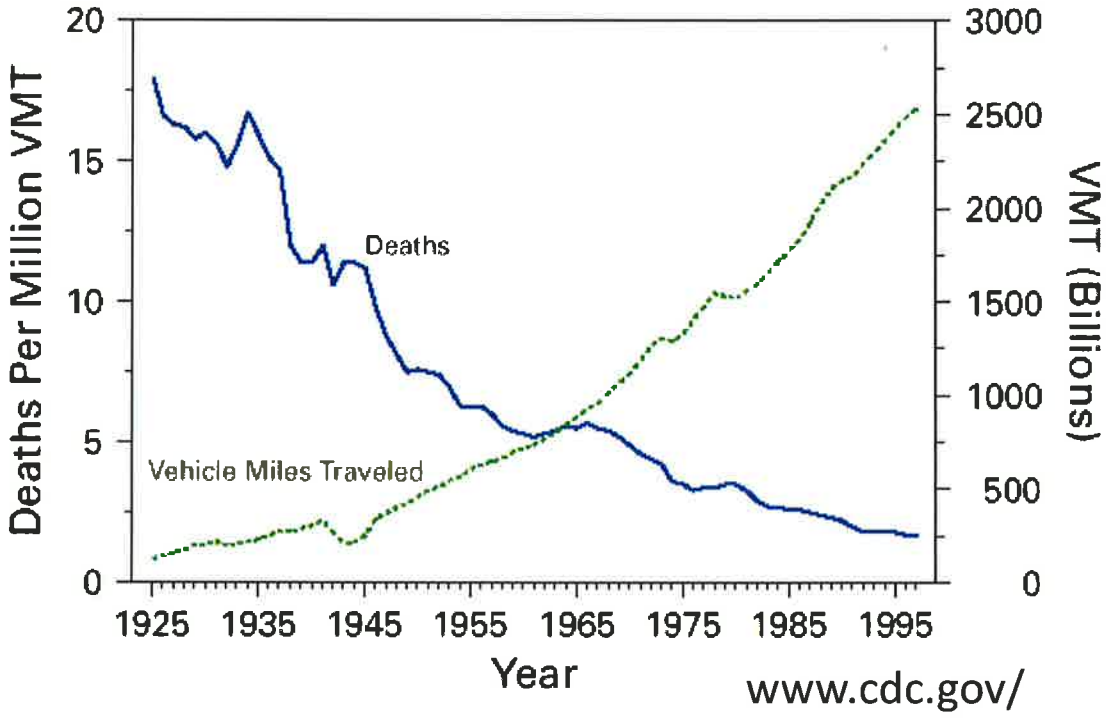
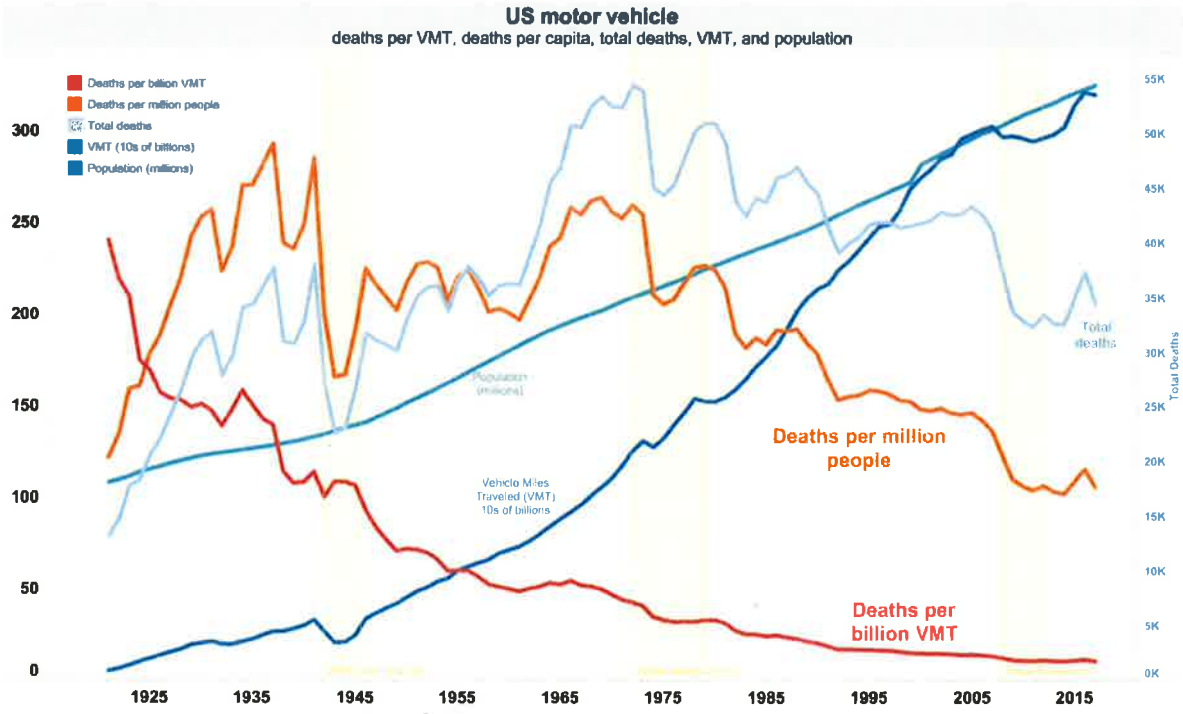
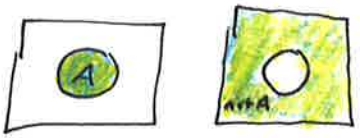


FIGURE 1. Motor-vehicle–related deaths per million vehicle miles traveled (VMT) and annual VMT, by year — United States, 1925–1997





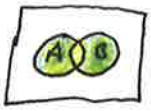
Probability



$P(A)$ = probability of event "A"

$P(A|B)$ = probability of event "A" given event "B" $= \frac{P(B|A)\,P(A)}{P(B)}$

$P(\text{not } A) = 1 - P(A) = P(\bar{A})$

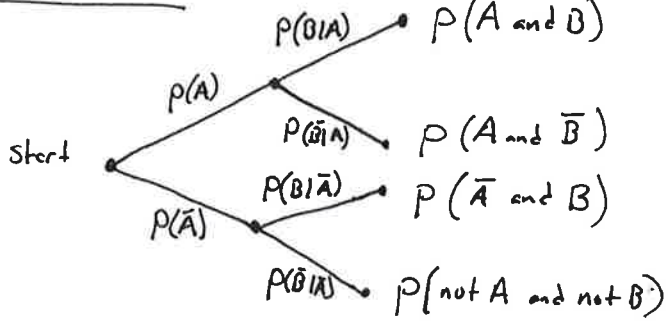


$P(A \cup B) = P(A) + P(B) - P(A \cap B) =$ A or B

$P(A \cap B) = P(A|B)\,P(B) = P(B|A)\,P(A) =$ A and B

Are A and B independent? Ex: The flap motor and the comm radio should be independent.... but what if lightning or a ham handed monkey for a mechanic?

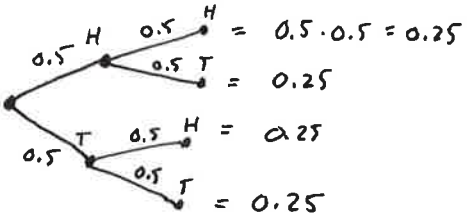
Probability Tree



Example: Independent coin toss

$P(A) = 0.5 \quad P(B) = 0.5$

$P(A|B) = P(A)$

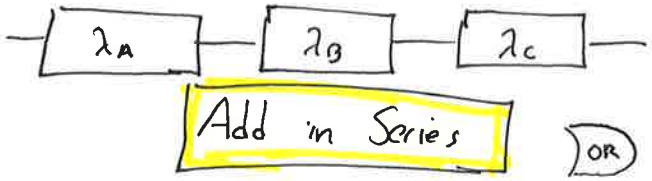


- What is the probability of two heads? $P(A \cap B) = P(A|B)\,P(B) = 0.5 \cdot 0.5 = 0.25$ ($P(A|B) = P(A)$)
- What is the probability of having a H and a T? (in no particular order)

$P(HT) + P(TH) = 0.5$

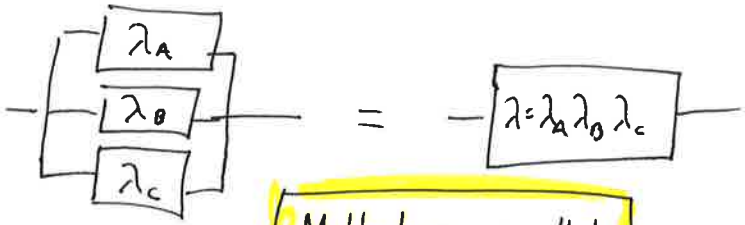
- What is the probability of TH? In order? 0.25

Reliability



Add in Series

OR



Multiply in parallel

AND

Ex: If $T_A = 1000$ hrs, $T_B = 2000$ hrs, $T_C = 3000$ hrs

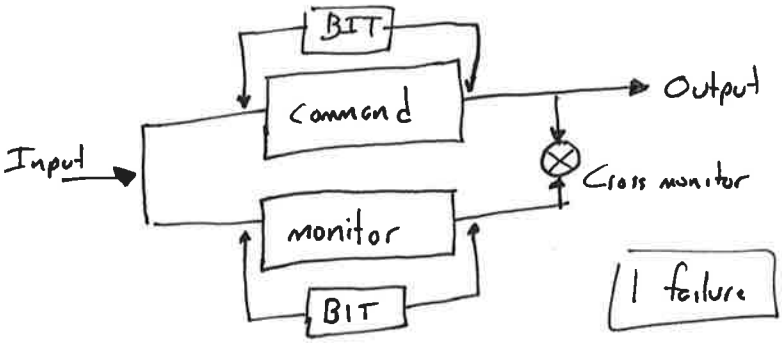
$\lambda_{series} = \frac{1}{1000} + \frac{1}{2000} + \frac{1}{3000} = 0.00183$

$T_{series} \approx 545$ hrs

$\lambda_{parallel} = \frac{1}{1000} \cdot \frac{1}{2000} \cdot \frac{1}{3000} = 1.67 \times 10^{-10}$

$T_{parallel} = 6 \times 10^{9}$ hrs (11 million times)

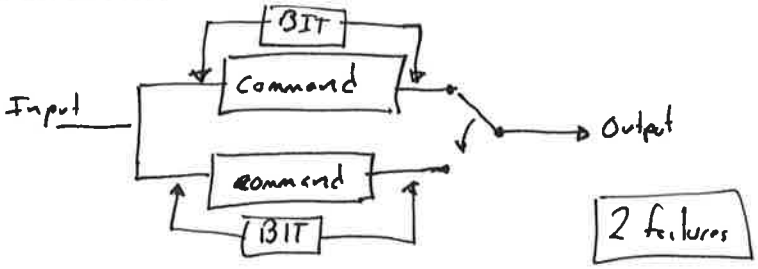
Cross monitor for Integrity



BIT ≡ Built-in test

λ_{XMON}	Output fails
λ_C	$\lambda_c + \lambda_m + \lambda_{XMON}$
λ_M	Fails to detect error
λ_B	$[\lambda_c(1-\lambda_B) + \lambda_m(1-\lambda_B)]\lambda_{XMON}$

Selection for Availability



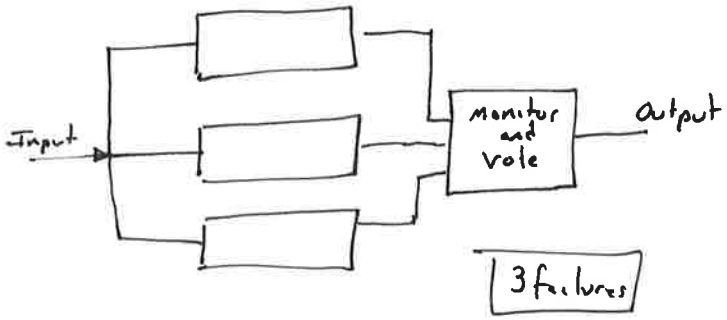
Output fails

$(\lambda_c)^2 + \lambda_s$

Fails to detect error

$2\lambda_c(1-\lambda_B)$

Voting



Space Shuttle had 5 separate systems voting.

Monitors + redundancy

Fault tree

Airbus FBW pitch

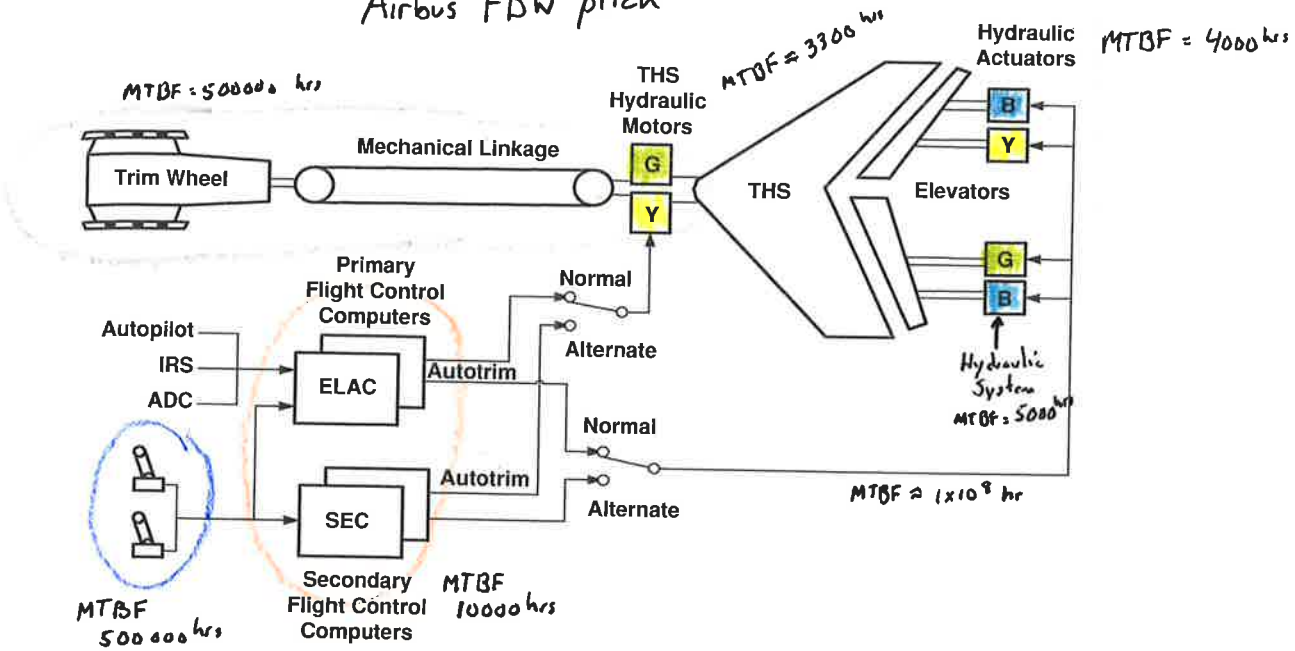


Figure A.1 Fly-by-wire flight control system – pitch axis

OR = Add

AND = Multiply

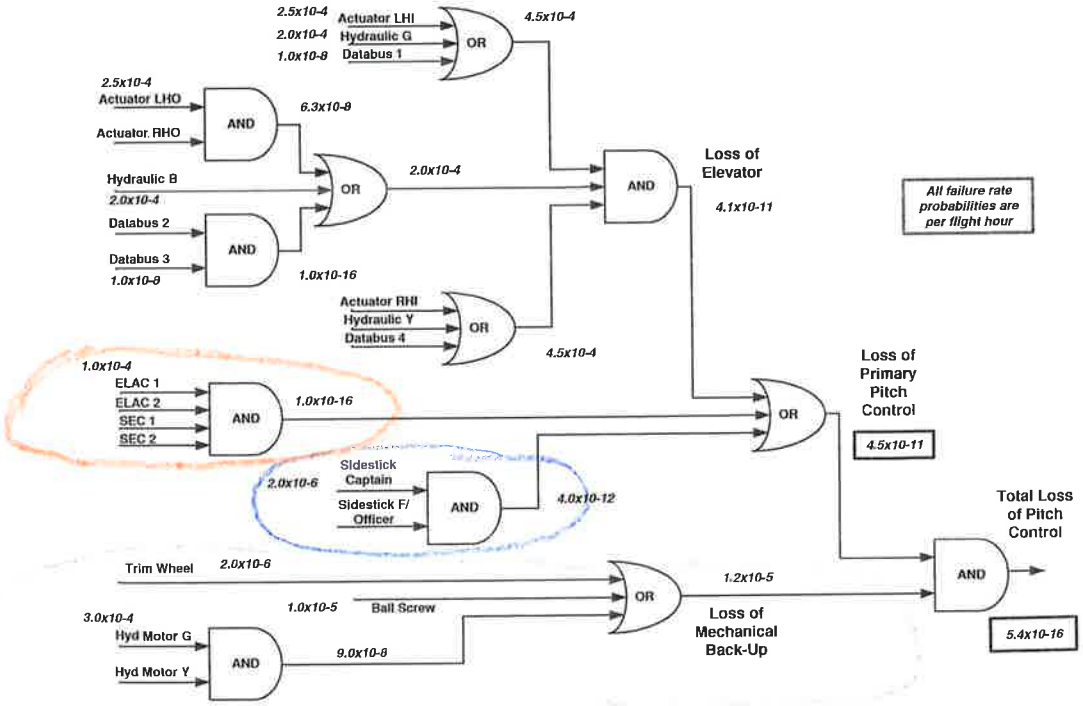


Figure A.3 Fly-by-wire flight control system – fault free diagram (simplified)

Source, CAS