FHA

Generic functions only.

No	Function	Functional failure	Failure condition	Flight phase	Effects	Classification	Ref	DAL
Sr. No.	* Provide something	Total Loss	at / during	Flying	Cannot use	NSE	Carrier	DAL E
	* Distribute -"-	Lesser		On ground	Crash	MIN	Action	DAL D
	Front -"-	More		Daytime	Accident	MAJ		DAL C
	Back -"-	Inadvertant		Night time	Unexpected	HAZ		DAL B
	* Switching	Erroneous		High speed	Malfunction	CAT		DAL A
	* Override function	Partial - front/rear		Low speed	Stress			
	* Indication	Always ON		Working	Control loss			
	* Human Machine Interface	Always OFF		Standstill	Explosion Ambiguity			

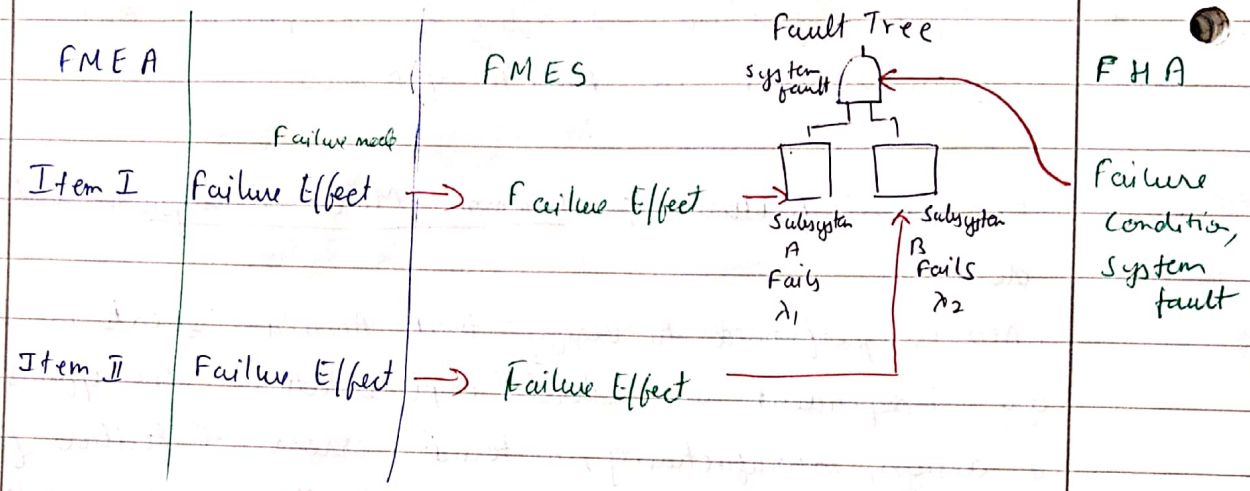
Piece part analysis - Material build - Single failure only

FMEA

No	Item	Function	Failure Mode	Failure rate	Failure Effects	Failure recognition	Remarks x
Sr no.	Each Item/ Component/ Part Separately.	Function of that part/ Item	short ckt open ckt broken/rupture ground over voltage under voltage lower more inadvertant erroneous always ON always OFF jammed	$\lambda_a, \lambda_b, \lambda_c$ $\lambda_{1.1}, \lambda_{1.2}$	1. Component 2. Subsystem 3. System * 1. Blow off * 2. Can't sense lesser, more * 2. } Total loss * 3. } Over, Under	Indicator Noticable Hidden Latent Hard movement noticable	1. condition influencing Effects 2. Compensat^n 3. Other info

FMES

Ref	Failure Mode	Failure Rate	Failure Effect	Detectability	Casual failure remarks
Sr No.	Total loss Over / under ~~Explosion~~ x (not included in single failure) generally	Summation of related λ	Next Level, system level effect accident, crash, control loss, Malfunction	Evident, Indicative Hidden, Latent	



- Single failure leading to more than one function loss in FMEA & FMES

→ For such failures, Common Mode Analysis should be done.

CMA is performed to verify that ANDed events in FTA/DD are independent in actual implementation. The effects of design, manufacturing, material errors & failure of system components which defeat their independence should be analyzed. Considerations should be given to the independence of functions & their respective monitors. Item with identical hardware and/or software could be susceptible to generic faults which could malfunction in multiple items.

Common mode faults can fall into several categories which should be analyzed. Eg of common mode faults:

- Hardware Errors
- Software Errors
- Hardware Failure
- Production/Repair flaw
- Installation Error
- Requirement Error
- Environmental factors
- Cascading fault
- Common mode Source faults.

- Owner sign for ? approver? authorizer?

four eye principle { Owner is signing for (Head of department) content of the document (not hiding, cheating)
approver - supervisor - for completeness & correctness (no wrong representation)
authorizes - No technical background, commercial guy (CEO) applicable for customer, authority, management point of view, applicability of document

- Verification & validation

review, walkthrough, inspection

Verification:- The evaluation of an implementation to determine that applicable requirements are met. Does not involve code execution

black box testing, whitebox testing, non functional testing

Validation- The determination that the requirements for a product are sufficiently correct & complete. Involves code execution.

Verification → software architecture, design & database, (early in development cycle)
Validation → actual software product, (software meets req, find bugs)

HALT HASS

HALT- • High accelerated life Test
- Development test to invoke failures in short time, identify reason & find corrective action.
- It applies high levels of stress for a short time to invoke the same failure modes which would appear with lower stress after a long time.
- Requires operation & monitoring of equipment during test.
- Test parameters- six axis vibration, temperature cycling, voltage variation
- "Test to fail"

HASS - High accelerated stress screen

- Production test to invoke those failures which are latent in the product due to the production process & detect them in a short time without reducing the useful life of the equipment.
- It requires operation & monitoring of the equipment during the whole test time
- It is Combination of all relavent stress parameters for time compression without reducing the useful life of the equipment.
- Detection of faults through functional testing
- Product monitored with high test coverage.

(HALT must be performed, uses screen profiles from HALT data)

Dormancy time & Risk time.

Dormancy time - Hidden failures inspected by maintainance (Hidden failure scenario). Time that shows how long the failure was hidden until it is finally detected

Risk time - The time in which the failure would lead to severe effects

This is usually associated with the final fault in a fault sequence leading to a specific failure condt

eg: Landing gear retraction system → Risk time during take off.

Cascading requirements

describe & trace in both direction

mapping between req & software for verification

Breaking down requirements from product level to system level down to equipment level. ~~product development life cycle~~

Generally requirements at the lower tier of the supply chain/ are fullfilled to satisfy the technical performances required by the tier above. Such cascading requirements is run sequentially from one tier to the next of supply chain/ design development phase

Requirements verification method.
Demonstration, Examinations, Test, Analysis

Increase in safety decreases reliability
To increase safety, redundant components/subsystems have to be introduced into the system. This implies more number of equipment are added to the system.
More equipments means more chances that equipments can break/malfunction & therefore reliability decreases

Random failure & error

Random failures = failures that can occur unpredictably during the lifetime of a hardware element, and that follow a probability distribution.
Caused by effects such as corrosion, thermal stressing, wearout. Generally caused due to physical causes.
These failures are non reproducable.
Error:- An occurance arising as a result of an incorrect action or decision by personal operating or maintaining a system. A mistake in specification, design, or implementation.

Active & passive safety

Active safety- Minimizes the probability of a crash.
eg- Antiskip system (ABS), Traction control (ESP), Power assisted brakes, Driver fatigue warning.

Passive safety- Minimizes the effect of crash
eg. Crumple zone, seat belts, belt tensioning, Air bag, roll over protection.

Π factors from MIL.

Π_E - Environmental factor - Defines environmental effect on failure rate

Π_Q - Quality factor

Π_V - Voltage stress factor.

stress $S = \frac{\text{operating voltage}}{\text{Rated voltage}}$

	Π_V		
S (Voltage stress)	Column 1	Column 2	Column 3
0·1	1·0	1·0	1·0
0·2	1·0	1·0	1·0
⋮	14	166	5·6

Thus if high rated voltage & low operating voltage, stress factor is less & Π_V is also less. Thus decrease failure rate

Π_T - Temperature factor: Generally lower ambient temp → Lower Π_T → low failure rate

Π_C - capacitance factor - smaller capacitance → smaller Π_C → low failure rate.

Failure rate by inservice experience

Confidence interval for in service experience is determined.

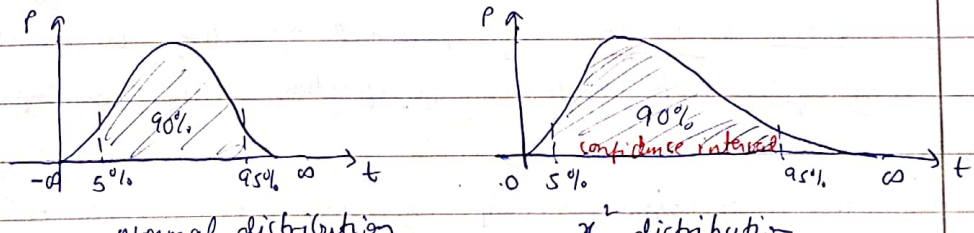
for small values of p_1, p_2, the quantile of x^2 (chi-square) distribution can be used to determine the confidence interval (p_1, p_2 are probabilities.)

(K → failures)

$$2K p_2 = x^2_{2(K+1),\,1-\alpha}$$

$$2K p_1 = x^2_{2K,\,\beta}$$

These equations cannot be used for $K = 0$ (i.e $K=0$ no failure observed)



Normal distribution x^2 distribution

Confidence interval is reduced to 0 to ∞ instead of -∞ to ∞

Technical safety & security

Technical safety:

Technical safety means the threat comes from the technical things designed by an engineer.

It focuses on safety in technical product design.

The failures are inherent to the system & they are because of the technical things designed by an engineer.

Such hazards should be identified & eliminated to make the product safe from causing injuries & significant material damage.

Security: If the threat comes from external things such as hackers, terrorists then it is a security threat.

Threat from intended person who wants to intrude something & destroy something.

Security measures shall be implemented to protect the system from such threats.

System failure & External event

System failure can occur because of hardware or software failure which leads to loss of function / malfunction of component, causing the system to freeze, reboot or stop functioning all together.

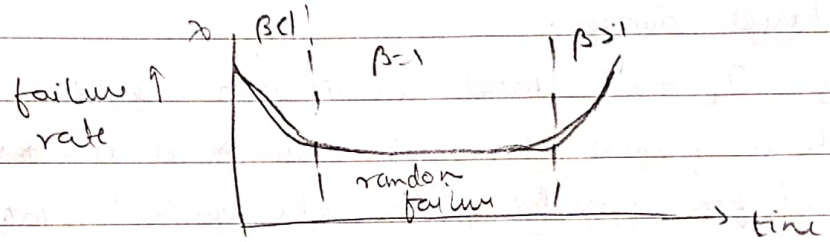
External event: an occurance which has its origin distinct from the system such as (for aircraft) → atmospheric conditions, (eg wind, temperature, lightning strikes), runaway conditions, cabin & baggage fires. This term is not intended to cover sabotage.

Segregation & separation:

Segregation: The maintenance of independence by means of a physical barrier between two hardware components.

Separation: The maintenance of independence by means of physical distance between two hardware components.

Bath tub curve



Bath tub curve is widely used in reliability engg. It describes a particular form of hazard function which comprises of three parts Describes it is a life characteristics. curve, which describes behaviour of failure rate over time.

Burn in phase $\beta < 1$

Initially failure rate is high but it is rapidly decreasing.

High initial failure rate is due to production problems.

This is called infant mortality.

Failures are due to → inadequate burn in
→ M/c assembly
→ quality problems

To make curve flatter
1) Better quality of material
2) Robust tests carried out
3) Error free setup.

β Constant phase $\beta = 1$
failure rate remains constant for longer period.
Usually caused by random failures probably by stress exceeding design strength.
To safety of service test is carried out in this phase & if the equipment is succesfully tested/serviced, its lifetime is extended.
(Regular maintainance is carried out)
The end point of this phase is called the designed service life.

Wear out phase $\beta > 1$
The failure rate increases as components begin to wear out due to fatigue, depletion of material, etc. wearout failure rate increases exponentially w.r.t. time

If maintainence is done before wear out phase, then its life characteristics will reach back to burn in phase

$\beta = 2$ Wear out
Linear increase of failure rate with time.

$\beta > 2$ old age wear out - Progressive increase of failure rate with time. Because of Bearings, corrosion.

Improve failure rate of capacitor.

for capacitor failure rate is given by

$$\lambda_p = \lambda_b \cdot \Pi_T \cdot \Pi_C \cdot \Pi_V \cdot \Pi_{SR} \cdot \Pi_Q \cdot \Pi_E \text{ failures}/10^6 \text{ Hours}$$

- λ_b — basic failure rate
- Π_T — Temperature factor
- Π_C — Capacitance factor
- Π_V — Voltage stress factor
- Π_{SR} — Series Resistance factor
- Π_Q — Quality factor
- Π_E — Environment factor

Basic failure rate is different for different types of capacitors eg - dielectric, electrolytic, ceramic.
can be choosen suitably to reduce λ_b

Π_T is lower for lower ↓ Temp.
If possible, reduce the ambient temperature of working area to reduce Π_T

Π_C is smaller for smaller capacitance values.

Π_V increases with ↑ S. Π_V depends on S. S is given by $S = \frac{\text{operating voltage}}{\text{Rated voltage}}$
So use Rated capacitor with much higher rated voltage than operating voltage.

Π_{SR} is more for lesser ↓ circuit resistance

$CR = \frac{\text{Resistance between caps of Power supply}}{\text{Voltage applied to capacitor}}$

D → 0.001
C → 0.01
S,B → 0.03
R → 0.1
P → 0.3
M → 1
L → 1.5

π_Q - D rated capacitors have lesser π_Q value
use established reliable rated capacitors

π_E - Depends on the working environment.

Reason for suspension to break

$\beta < 1$

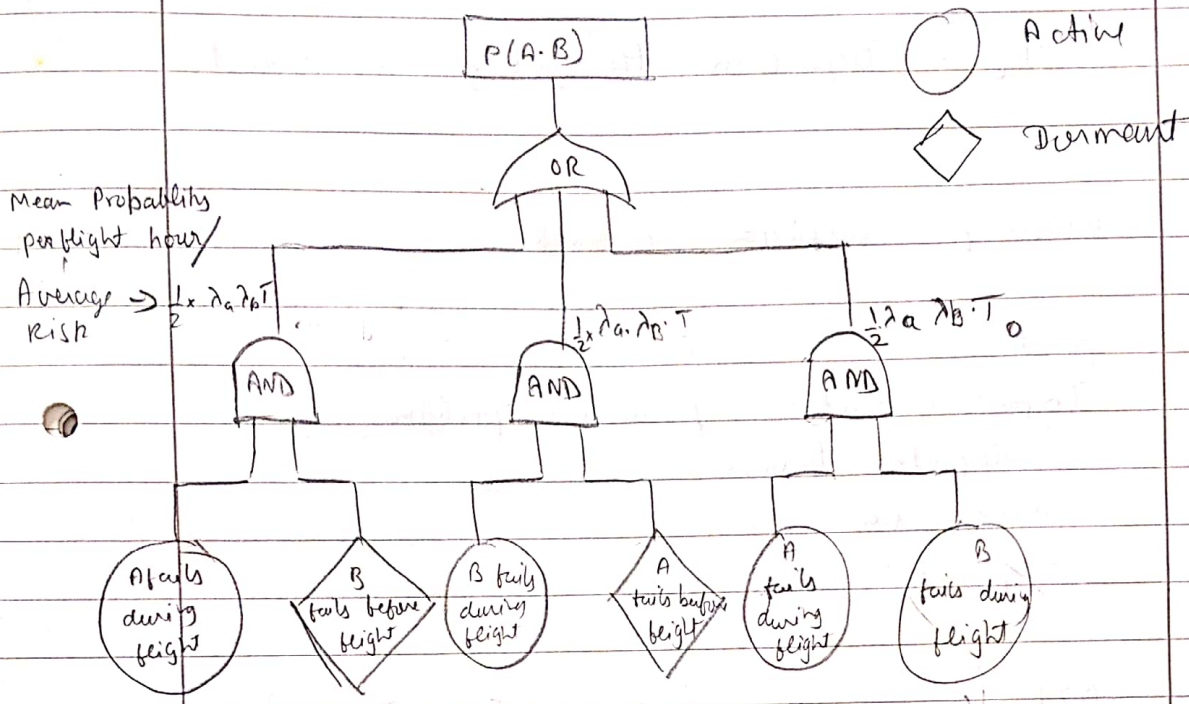
Infant mortality - production problem
- inadequate burn in
- misassembly
- quality problem

$\beta > 1$

Wear out, Not serviced/maintained properly, corrosion of bearing problem., Mishandling

Calculation of hidden failures:

Double failure, mean flight time T_0, Inspecting interval T, $T \gg T_0$.



Consider i^{th} failure during operation cycle no.

Case 1: B fails before flight, A fails during flight $T = NT_0$

$$P_1 = \lambda_a T_0 \lambda_b i T_0 = \lambda_a \cdot \lambda_b i T_0^2$$

Case 2: A fails before flight, B fails during flight

$$P_2 = \lambda_a i T_0 \lambda_b T_0 = \lambda_a i \lambda_b T_0^2$$

Case 3 - A fails during flight, B fails during flight

$$P_3 = \lambda_a T_0 \lambda_b T_0 = \lambda_a \lambda_b T_0^2$$

Total probability of flight: $P(A \cdot B) = P_1 + P_2 + P_3$

$$= \lambda_a \lambda_b i T_0^2 + \lambda_a i \lambda_b T_0^2 + \lambda_a \cdot \lambda_b T_0^2$$

$$P(A \cdot B) = \lambda_a \cdot \lambda_b \cdot T_0^2 (2i + 1)$$

Mean probability per flight hour is given by

$$P_{avg} = \frac{1}{NT_0} \sum_{i=1}^{M} \left[\lambda_a \cdot \lambda_b \cdot T_0^2 (2i+1) \right]$$

$$= \frac{\lambda_a \cdot \lambda_b T_0^2}{NT_0} \sum_{i=1}^{N} (2i+1)$$

$$= \frac{\lambda_a \cdot \lambda_b \cdot T_0}{N} \cdot 2 \sum_{i=1}^{N} \left(i + \frac{1}{2} \right)$$

$$= \lambda_a \cdot \frac{\lambda_b \cdot T_0 \cdot 2}{N} \cdot \frac{N(N+1)}{2} + \frac{1}{2}$$

$$= \lambda_a \cdot \lambda_b \cdot T_0 \cdot N$$

$N \gg 1$

$\therefore N+1 \approx N$

$$\sum_{i=1}^{N} i = \frac{(N+1)N}{2}$$

Probability $P(A \cdot B)$

(first flight after inspection): $i = 1$

Case 1: B hidden, A active

$P_x = \lambda_a T_0 \lambda_b T_0 = \lambda_a \lambda_b T_0^2$

Case 2: A hidden, B active

$P_y = \lambda_a T_0 \lambda_b \cdot T_0 = \lambda_a \cdot \lambda_b T_0^2$

Case 3: A active, B active

$P_z = \lambda_a \cdot T_0 \lambda_b T_0 = \lambda_a \lambda_b T_0^2$

Mean probability: $P(A \cdot B) = \frac{P_x + P_y + P_z}{N} = 3 \lambda_a \lambda_b T_0^2$

$= \frac{1}{N} \sum_{i=1}^{N} P_i$

Mean Probability per hour $= \frac{1}{NT_0} \sum_{i=1}^{N} (P_x + P_y + P_z) = 3 \lambda_a \lambda_b T_0$

Last flight before inspection

Case 1

$P_x = \lambda_a T \lambda_b \cdot T = \lambda_a \lambda_b N T_0^2$

Case 2

$P_y = \lambda_a T \lambda_b T_0 = \lambda_a \lambda_b N T_0^2$

Case 3

$P_z = \lambda_a \lambda_b T_0^2 N^2$

$P(A \cdot B) = \frac{P_x + P_y + P_z}{N}$

$= \lambda_a \lambda_b N T_0 \frac{(2T_0 + T_0)}{N} (2N+1)$

$= \lambda_a \lambda_b T_0 (3T_0)$

$= 3 \lambda_a \lambda_b T_0^2 N$