ROLE OF ASSURANCE TECHNOLOGIES IN A/C DESIGN

Kota Harinarayana

Assurance technologies are the processes for assuring that a product performs well during its life time.

Assurance Technologies

Performance effectiveness, one of the key constituents of ***systems engineering,*** totally relies on **Assurance Technologies**

Assurance Technologies

BENEFITS

Product Realization

- Better
- Faster
- Cheaper

Assurance Technologies

RELIABILITY

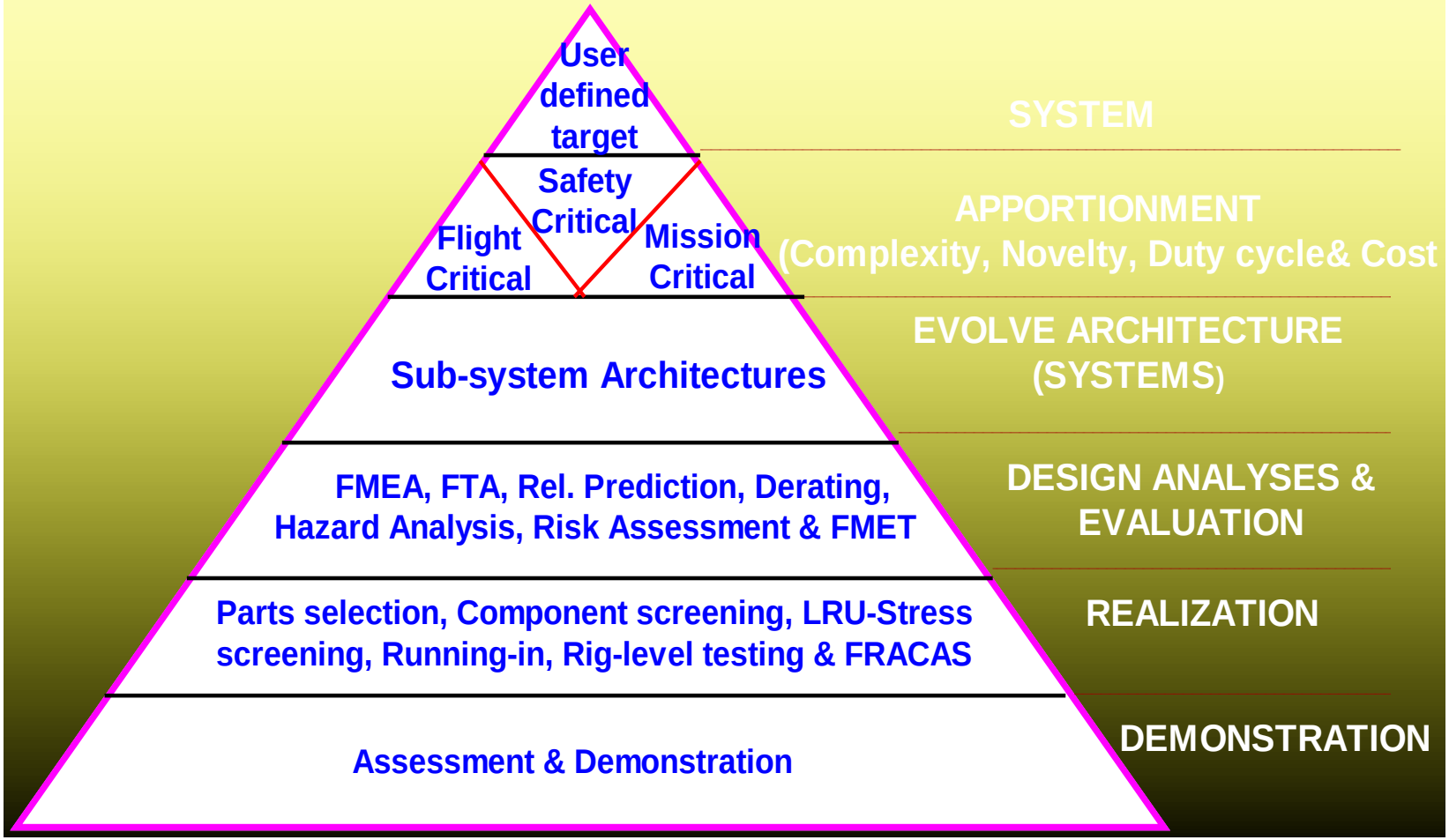
Importance of Reliability

- Mission accomplishment
- Operational readiness (Availability)
- To operate with lean logistics
- To reduce ownership cost

Phases for reliability

- Design for Reliability
- Identification of errors and obviating them during production
- Measure, Monitor and Correct to enable reliability growth

RELIABILITY IN DESIGN



Reliability Targets

Reliability targets are defined:

- Either by user
- Or by the organization (keeping pace with the competitive product market)

Reliability Apportionment

The reliability defined for the system is apportioned to its individual sub-systems by:

- AGREE method (MTBF based)
- ARINC method (failure rate based)
- KARMIOL method (feasibility of objectives based)
- Equal apportionment (when no insight is available)

Reliability specification

Typical reliability specification shall contain

- Reliability goals
- Functional and interface requirements
- Operational environment
- Life span (storage and operating)
- Stress / fatigue spectrum
- Servicing requirements
- Test requirements with accept / reject criterion

- Estimated From field failure
- Predicted data from Modeling
- Vendor supplied data
- Mil HDBK 217F for electronic parts & NPRD (for non electronics parts) data from RADC

Sources For Failure Rate Data (With order of preference)

AIRCRAFT RELIABILITY GOAL

Sl No.	Aircraft	Reliability Goal	Remarks
1	Jaguar	0.9	
2	Tornado	0.95	
3	F111 A	0.85	Achived 0.86 after 4 years [0.6-during Dev Testing, 1965 0.85 After Pilot Training, 1967 0.90 Operational Usage, 1969]
4	F 18	3.7 MFHBF, 0.9 [Maintainability-11 MMH/FH & MTTR 1.76 Hrs]	•Achieved 2.0 after 1200 FH & 3.7 demonstrated during FSD •0.8 with special 50 flight A/C test (Demonstrated at FSE) •Maintainability demonstrated at FSE
6	F 16	0.9, 2.9 MFHBF	Achieved 0.85 during Dev Phase [1.75 MFHBF demonstrated during development]

SYSTEM WISE RELIABILITY GOAL

Sl No	Aircraf	System	R Goal		Remarks
			Development	Production	
1	F 16	Airframe	3.5 MFHBF	6.1 MFHBF	
		Propulsion Plant	27.0 MFHBF	66.0 MFHBF	
		Avionics	5.7 MFHBF	8.3 MFHBF	
		Armament	65.0 MFHBF	85.0 MFHBF	
		Weapon Delivery	710 MFHBF	940 MFHBF	
		FCS	18.0 MFHBF	30.0 MFHBF	
		Radar	60 MFHBF	100 MFHBF	
2	F 18	Radar	80 Hrs MTBF (50th Unit)	- - - -	
			100 Hrs MTBF (100th Unit)	- - - -	Demonstrated on 125th Unit
		Avionics	30 Hrs MTBF	Fleet Analysis	Demonstrated 1 YR after FSE

Reliability Techniques

- Zero failure / safe margin design
- Fault tolerant / damaged tolerance design
- Reliability allocation, prediction and modeling
- Reliability analysis through FMECA / FTA
- De-rating
- Robust design
- Design reviews and audit

SYSTEMWISE RELIABILITY

Target Reliability > 0.95 for one hour sortie (As per ASR)

Sl. No.	System	Mission Reliability			
		Ref. Aircraft	Apportioned	Reapportioned	Predicted
1	Airframe	0.999900	0.999900	0.99990	0.99990
2	Flight Control System	0.994415651	0.9975031	0.99900	0.99939
3	Avionics	0.9720	0.9720	0.97200	0.97200
4	Propulsion	0.996860	0.9964349	0.99643	0.99643
5	Secondary Power System	0.99929	0.9982542	0.99825	0.997039
6	Environment Control System	0.999865	0.9973874	0.99738	0.997188
7	Liquid Oxygen System	0.999955	0.9994071	0.99940	0.999242
8	Elect. Power Gen. System	0.99898	0.9973311	0.99898	0.99929
9	Hyd. Power Gen. & Distribution System	0.99939	0.9968385	0.99939	0.9993517
10	Aircraft fuel system	0.99723	0.9974661	0.99747	0.9982127
11	Fire Extinguisher System	0.99993	0.9993548	0.99936	0.99936
12	Crew Escape System	-	0.9993379	0.99934	0.99934
13	L/G, W/B System, NW steering & Brake Parachute System	0.99839	0.9980881	0.99809	0.99809

Weightage Factors for Apportionment

Sl. No.	System	Complexity (K_i)	Stat e of Art (S_i)	Mintainability (m_i)	Duty Cycle (D_i)	Criticality (Cr_i)	Redundancy Level (R_i)
1	Airframe	9	2	6	1	9	1
2	FCS	9	8	9	1	9	4
3	Electrical System	5	6	8	1	9	4
4	Mission Management System	7	8	9	1	7	2
5	Propulsion	9	9	6	1	9	1
6	Fuel System	7	4	6	1	8	1
7	Communication System	9	8	8	1	8	2
8	Hydraulic System	4	6	8	1	8	2
9	ECS & Oxygen	4	4	8	1	6	1
10	Landing Gear	7	2	8	0.067	9	1
11	Brake and NWS	7	4	8	0.067	9	2
12	Navigation System	6	8	9	1	8	2
13	Payload / Stores	9	6	6	0.003	6	1

Apportionment of Reliability

Sl. No.	System	Redundancy	Apportioned Reliability	MTBF
1	Airframe	1	0.9990005	1000
2	FCS	4	0.9980019	500
3	Electrical System	4	0.9980787	520
4	Mission Management System	2	0.9964349	280
5	Propulsion	1	0.9990005	1000
6	Fuel System	1	0.9981149	530
7	Communication System	2	0.9968798	320
8	Hydraulic System	2	0.9980787	520
9	ECS & Oxygen	1	0.9976218	420
10	Landing Gear	1	0.9977298	440
11	Brakes & NWS	2	0.9978284	460
12	Navigation System	2	0.9972260	360
13	Payload / Stores	1	0.9973718	380
OVERALL SYSTEM RELIABILITY – 0.972				

Elements of Best Practices

- Understanding the Failure (Physics of Failure)
- Consideration of deployment environment
- Appropriate parts and material selection
- Adoption of robust design technique
- Judicial application of redundancy
- Institution of Review mechanism
- Development testing (TAAF)
- Reliability assertion (Qualitative and Quantitative)

General Constraints / Limitations

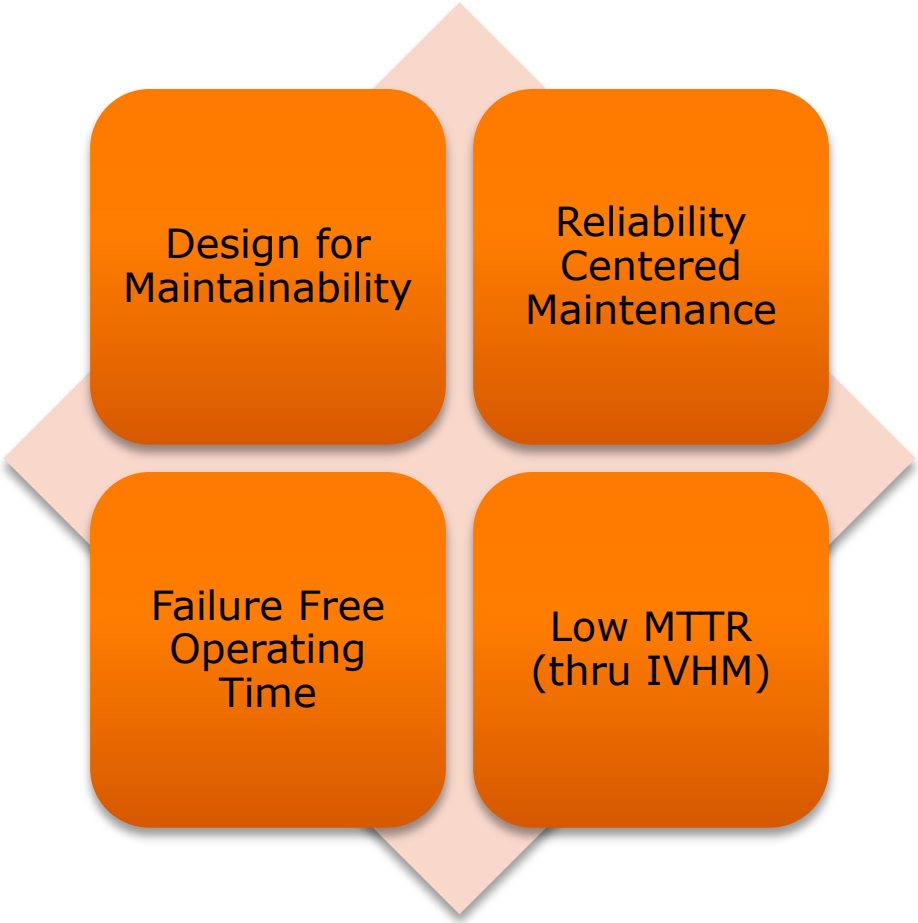
- Domination of cost and schedule considerations
- Inadequate resources / budgeting for failure analysis and corrective actions
- Improper understanding / assumptions of stresses and environment
- Setting forth of optimistic goals

MAINTAINABILITY

Definition of Maintainability

Maintainability is the science of minimizing the need for maintenance and minimizing the down time if maintenance action is necessary. The figure of merit for maintainability are

- High inherent availability
- Low mean down time for maintenance
- Low equipment repair time



Elements of Maintainability

- Maintainability Goals
- Maintainability Estimation
- Design for Maintainability
- Logistics Features (Support Tools, Spares and Documentation)
- Maintainability Demonstration

Means for Maintainability

Process for Maintainability

1. Maintainability specification
   (MTTR, Replacement time and Servicing requirements)
2. Maintainability Analysis
3. Maintainability Prediction
4. Design for Maintainability

Part name / Part No.	Potential Failure Modes	Causes (Failure Mechanism)	Effects	Expected Down-time	Frequency Per Year	Recommended Improvement	Maintenance Requirements
Pipe	Leakage in pipe	1. Corrosion	Loss of Freon	8 h	2	Use stainless s steel pipe	None
		2. Temp. cycling	Loss of Freon	8 h	5	Monitor temp. with thermocouples	Replace probes every 120 days
	Leakage at the joint	1. Cumulative Fatigue	Loss of Freon	14 h	4	Monitor vibration with accelerometers	Calibrate accelerometers semi-annually
		2. Poor soldering	Loss of Freon	2 h	2	Provide flexible plaster coupling at the joint	None
Valve	Sticky, intermittent	1. Dirt or foreign objects	Loss of control of temperature	5 h	2	Electronic redundant valve action and fault identification	Clean every 15 days
	Stuck open	1. Component wear out	Loss of control of temperature	4 h	1	Electronic redundant valve action and fault identification	Check every 3 months
	Stuck closed	1. Component failed	Loss of control of temperature	4 h	2	Electronic redundant valve action and fault identification	Check every 3 months
		2. Component expansion and contraction	Loss of control of temperature	5 h	3	Electronic redundant valve action and fault identification	None

An Example of FMECA for Maintainability

- Accessibility
- Inspectability
- Testability (BIT,Test connectors &Test equipments)
- Interchangeability
- Standardization
- Modularity (SRU, LRU concepts)
- Repairability / Serviceability
- Supportability

Design for Maintainability

EVOLUTION OF MAINTAINABILITY FEATURES IN FIGHTER AIRCRAFT

.	MIRAGE 2000	LCA
		• MMH/FH≅ 20 (ESTIMATE)
		• SCHEDULED MAINT REDUCED TO MIN.
		• INTEGRATED ON-CONDITION MAINT.
MiG - 21	• MMH/FH≅ 40	• POSITIVE FAULT LOCALISATION UPTO LRU LEVEL
	• SCHEDULED MAINT. OF STRUCTURE	• POWER ON SELF TEST (POST)
• MMH/FH≅ 140	• SCHEDULED MAINT. OF GEN SYS	• HEALTH MONITORING OF GENERAL SYSTEMS THRO' USMS
• CONVENTIONAL SCHEDULE MAINT	• ON CONDITION MAINT OF AVIONICS	• MILKING OF HEALTH DATA THRO' MPRU
• NO BUILT IN TEST PROVISION	• BIT FOR AVIONICS	• C-BIT, P-BIT AND M-BIT FOR FAULT DIAGNOSIS WITHOUT EXTERNAL AIDS
• NO FAULT LOGGING	• LOGGING OF IN-FLIGHT FAILURES	
• ACCESS PANELS 20% OF SURFACE AREA	• ACCESS PANELS – 30% OF SURFACE AREA	• ACCESS PANELS – 35% OF SURFACE AREA
• LIMITED ACCESSIBILITY OF LRUs	• IMPROVED ACCESSIBILITY OF LRUs	• REDUCED NO OF LRUs • IMPROVED ACCESSIBILITY FOR LRUs
• TELLTALE INDICATORS	• TELLTALE INDICATORS • MODULAR DESIGN	• TELLTALE INDICATORS • MODULAR DESIGN
• ENGINE REMOVAL: - 12 HRS - HORIZONTAL MODE - SPLIT FUSELAGE	• ENGINE REMOVAL - 4 HRS - HORIZONTAL MODE - REMOVABLE TAIL CONE	• ENGINE REMOVAL - 30 MINUTES - VERTICAL MODE -ACCESS PANELS ONLY
• FAIL SAFE DESIGN FOR STRUCTURE	• FAIL SAFE DESIGN FOR STRUCTURE	•DAMAGE TOLERANT DESIGN FOR STRUCTURE

DESIGN FOR ACCESSIBILITY AND EASE OF MAINTAINANCE

ACCESSIBILITY MEANS HAVING SUFFICIENT ROOM AROUND A COMPONENT TO DIAGNOSE, TROUBLESHOOT AND CARRY OUT COMPLETE MAINTENANCE WORK IN A SAFE AND EFFECTIVE MANNER. PROVISION MUST BE MADE FOR MOVEMENT OF NECESSARY TOOLS AND EQUIPMENT WITH CONSIDERATION FOR VARIOUS BODY POSITIONS.

NORMAL PRACTICE IS TO MAKE MOCKUPS TO STUDY ACCESSIBILITY. OF-LATE DIGITAL MOCKUPS AND VIRTUAL REALITY HAVE BECOME VERY EFFECTIVE TOOLS TO STUDY ACCESSIBILITY

DESIGN FOR EASE OF MAINTENANCE:

EASE OF MAINTENANCE MEANS MAKING ACTIVITIES AT THE HUMAN / EQUIPMENT INTERFACE EASIER. IT CAN BE ASSURED MANY WAYS:

- ***MINIMISE MAINTENANCE IN THE FIRST PLACE***
- ***ALLOW REPAIRS WITH LEAST HANDLING***
- ***DESIGN FOR RELIABILITY OF THE INTERFACE OF MAKING PARTS***
- ***DESIGN FOR OFF LINE REPAIR***
- ***PROVIDE FAULT TOLERANCE***
- ***PLAN TOOLS AND EQUIPMENT IN ADVANCE***
- ***DESIGN FOR REMOVE AND REPLACE INSTEAD OF REPAIR***
- ***USE AUTOMATED TEST EQUIPMENT***
- ***DESIGN FOR TESTABILITY***
- ***ADOPT MODULAR DESIGNS***
- ***DESIGN FOR WORKING ENVIRONMENT***
- ***ADOPT STANDARDISATION***
- ***DESIGN FOR INTERCHANGEABILITY***

CRITERIA FOR ACCESSIBILITY ASSESSMENT

SL. NO.	CRITERIA	RATING
1.	ACCESS ADEQUATE BOTH FOR VISUAL AND MANIPULATIVE TASKS	4
2.	ACCESS ADEQUATE FOR VISUAL AND MANIPULATIVE TASKS WITH SPECIAL GSE / STAND	3
3.	ACCESS ADEQUATE FOR MANIPULATIVE TASKS BUT NOT FULLY VISIBLE	2
4.	ACCESS ADEQUATE FOR VISUAL BUT NOT FULLY MANIPULATIVE	1
5.	ACCESS INADEQUATE FOR VISUAL OR MANIPULATIVE TASKS	0

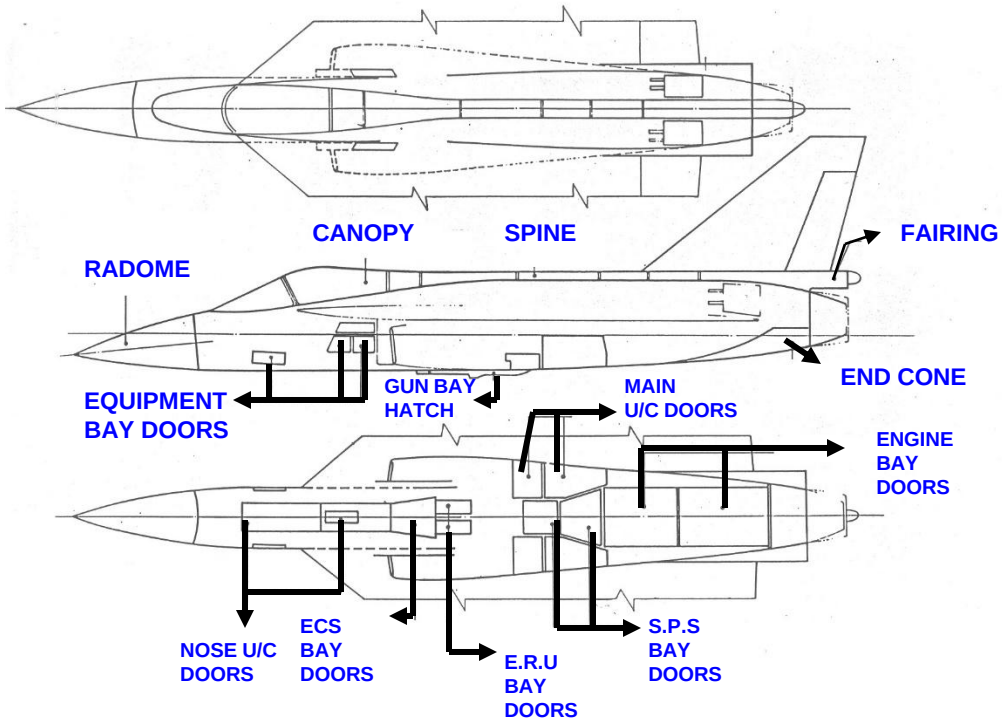
CRITERIA FOR ASSESSING TYPES OF FASTENERS AND SPECIAL TOOLS REQUIRED

SL. NO.	CRITERIA	RATING
1.	FASTENERS ARE CAPTIVE, NEED NO SPECIAL TOOLS AND REQUIRE SIMPLE PROCEDURES FOR REMOVAL AND INSTALLATION	4
2.	FASTENERS NEED SPECIAL TOOLS AND REQUIRE SIMPLE PROCEDURES FOR REMOVAL AND INSTALLATION	3
3.	FASTENERS NEED NO SPECIAL TOOLS AND REQUIRE COMPLEX PROCEDURES FOR REMOVAL AND INSTALLATION	2
4.	FASTENERS NEED SPECIAL TOOLS AND REQUIRE COMPLEX PROCEDURES FOR REMOVAL AND INSTALLATION	1

DEFINITION OF COMPLEX PROCEDURE:

-NEEDS ADDITIONAL PROCEDURE SUCH AS PRE-CHILLING, ETC.,
-NEEDS REMOVAL OF OTHER ITEMS
-REQUIRES MORE THAN ONE PERSON TO HANDLE

DOORS & HATCHES



OVERALL ACCESSIBILITY SCORING OF LCA TD1

SL. NO.	ITEM	OVERALL ACCESSIBILITY SCORING	FREQUENCY OF REMOVAL	CONCLUSION
1.	WING TO FUSELAGE	3.4	C	GOOD
2.	UNDERCARRIAGE			
	NOSE U/C	3.9	C	GOOD
	MAIN U/C	3.7	C	GOOD
3.	ENGINE TO FUSELAGE	3.0	A	GOOD
4.	VERTICAL TAIL FUSELAGE	3.6	C	GOOD
5.	AMAGB ATTACHMENT	3.7	A	GOOD
6.	RADOME ASSEMBLY TO FUSELAGE	4.0	A	GOOD
7.	SLATS TO WING	4.0	C	GOOD
8.	ELEVONS TO WING	3.5	C	GOOD
9.	RUDDER TO FIN	3.6	C	GOOD
10.	CANOPY TO FUSELAGE	4.0	C	GOOD
11.	GUN ATTACHMENT	3.2	A	GOOD
12.	PYLONS TO STRUCTURE	3.2	A	GOOD
13.	DOORS, CUTOUTS & HATCHES	--	A	GOOD
14.	AIRBRAKE TO FUSELAGE	3.5	C	GOOD
15.	SEAT TO FUSELAGE	3.1	B	GOOD

FREQUENCY OF REMOVAL

A. LESS THAN 100 HOURS
B. BETWEEN 100-400 HOURS
CONSIDERED AS GOOD
C. AT OVERHAUL OR AS REQUIRED

ACCEPTANCE CRITERIA

3-4 CONSIDERED AS GOOD
2-3
1-2 CONSIDERED AS GOOD

IVHM

Integrated Vehicle Health Monitoring (IVHM) is a contemporary feature for both diagnostics and prognostics of Condition Based Monitoring (CBM) to predict Remaining Useful Life (RUL) by application of failure propagation model, tracking of usage history and degradation trending to obtain enhanced availability and cost advantage

- Fault detection
- Fault isolation
- Advanced diagnostic
- Predictive prognostic
- Time to failure model
- Component usage tracking
- Degradation trending
- False alarm mitigation
- Health reporting
- Aid for decision making
- Information Fusion

Activity

Function	Models
Reliability Prediction	RBD (MTBF)
FMECA	Mil 1629/SAE J1739
FTA	Fault/Event tree
Reliability Growth Analysis	Weibull
Reliability Magt.	FRACAS
Maintainability Prediction	Mil Hdbk 472 (MTTR)
Maintainability Simulation	Markov
Maintenance Planning	MSG 3

Software Tools

- **ITEM**
- **Relex**
- **ReliaSoft**
- **RAM Commander**

Software Tools for R&M

HUMAN FACTORS AND VALUE ENGINEERING

Error due to	Error due to
Substitution	Haste
Selection	Sequencing
Reading	Over confidence
Irritation	Reversal
Warning	Unintentional activation
Lack of Alertness	Oversight and Omission
Lack of Understanding	Casual Behavior

Influences on Human Factors

- Integrated Product Development
- Design for Manufacturability
- Design to Cost
- Lean Manufacturing
- Efficient Supply Chain Integration

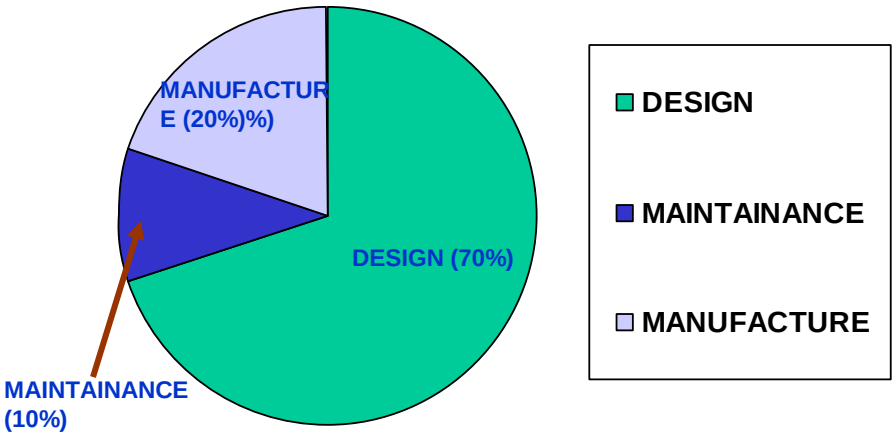
Elements of Value Engineering

Quality Assurance

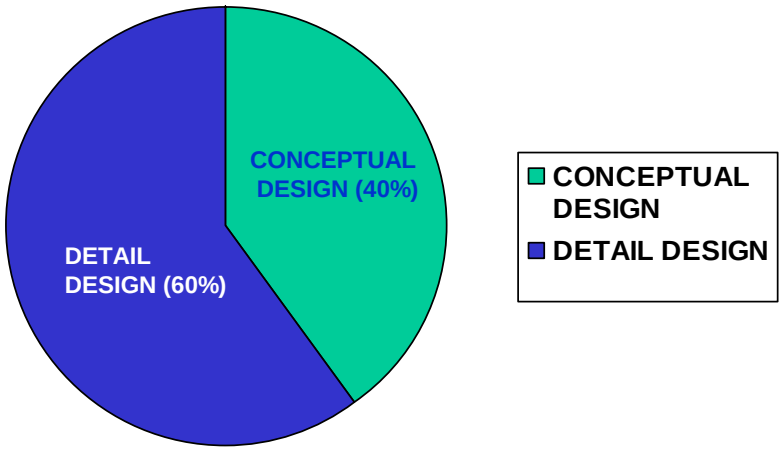
Quality assurance is a mechanism to ensure the process followed from concept to retirement to realize a product is right at all the time, by use of various tools and techniques.

Quality Assurance (QA)

QUALITY - MAJOR INFLUENCING FACTORS

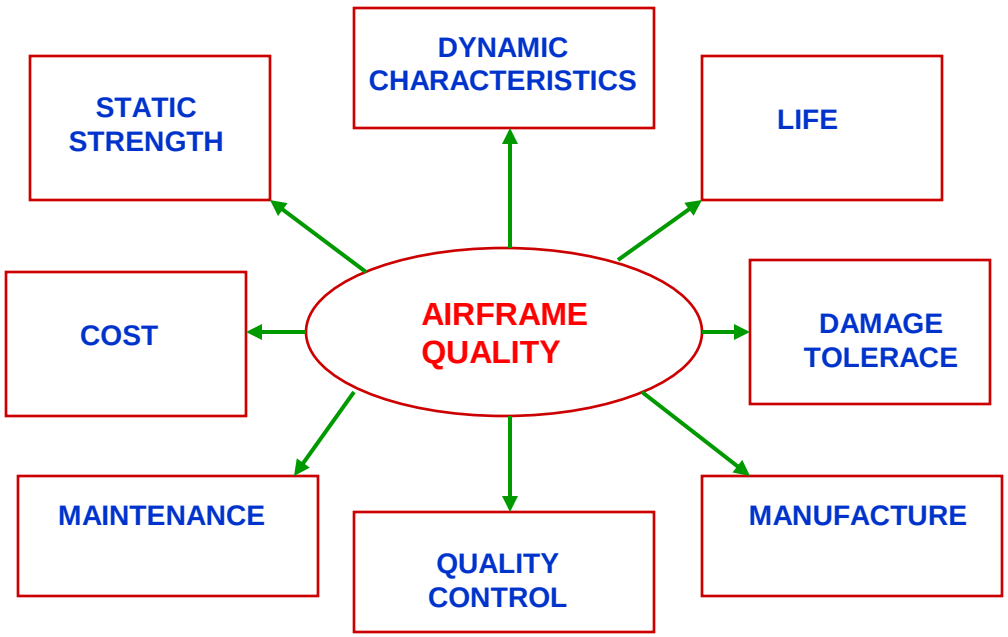


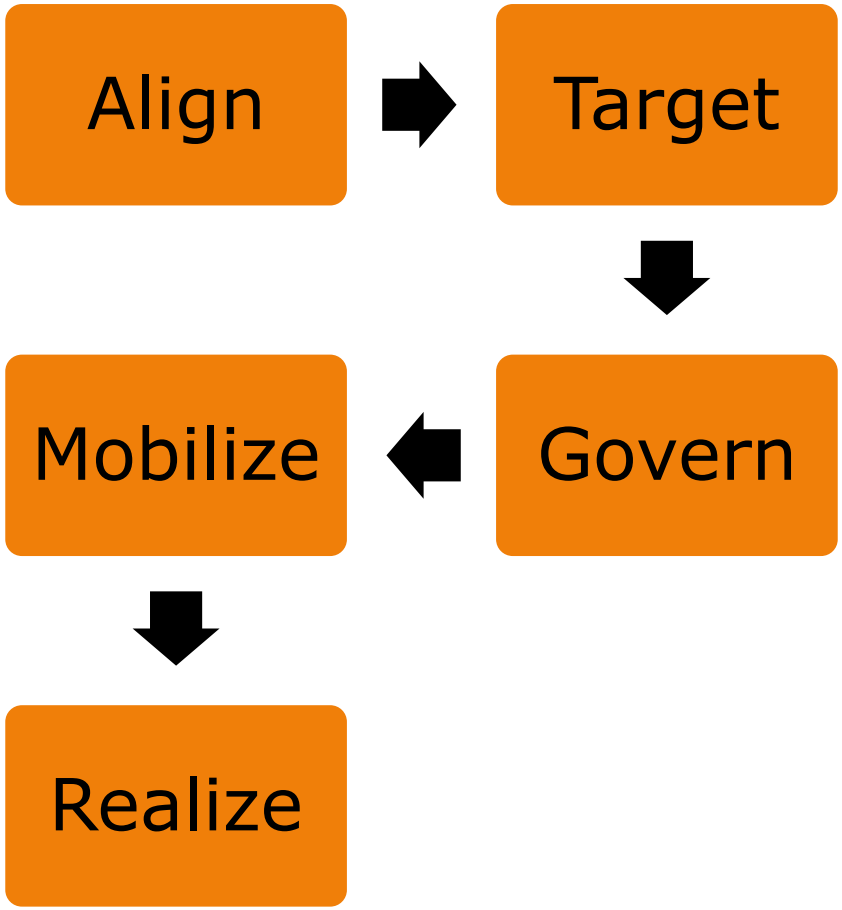
QUALITY BY DESIGN



AIRFRAME QUALITY

AIRFRAME PERFORMS AS SPECIFIED DURING THE REQUIRED LIFE TIME WHEN USED AS INTENDED WITH PROPER MAINTAINANCE WITHOUT ANY FAILURE





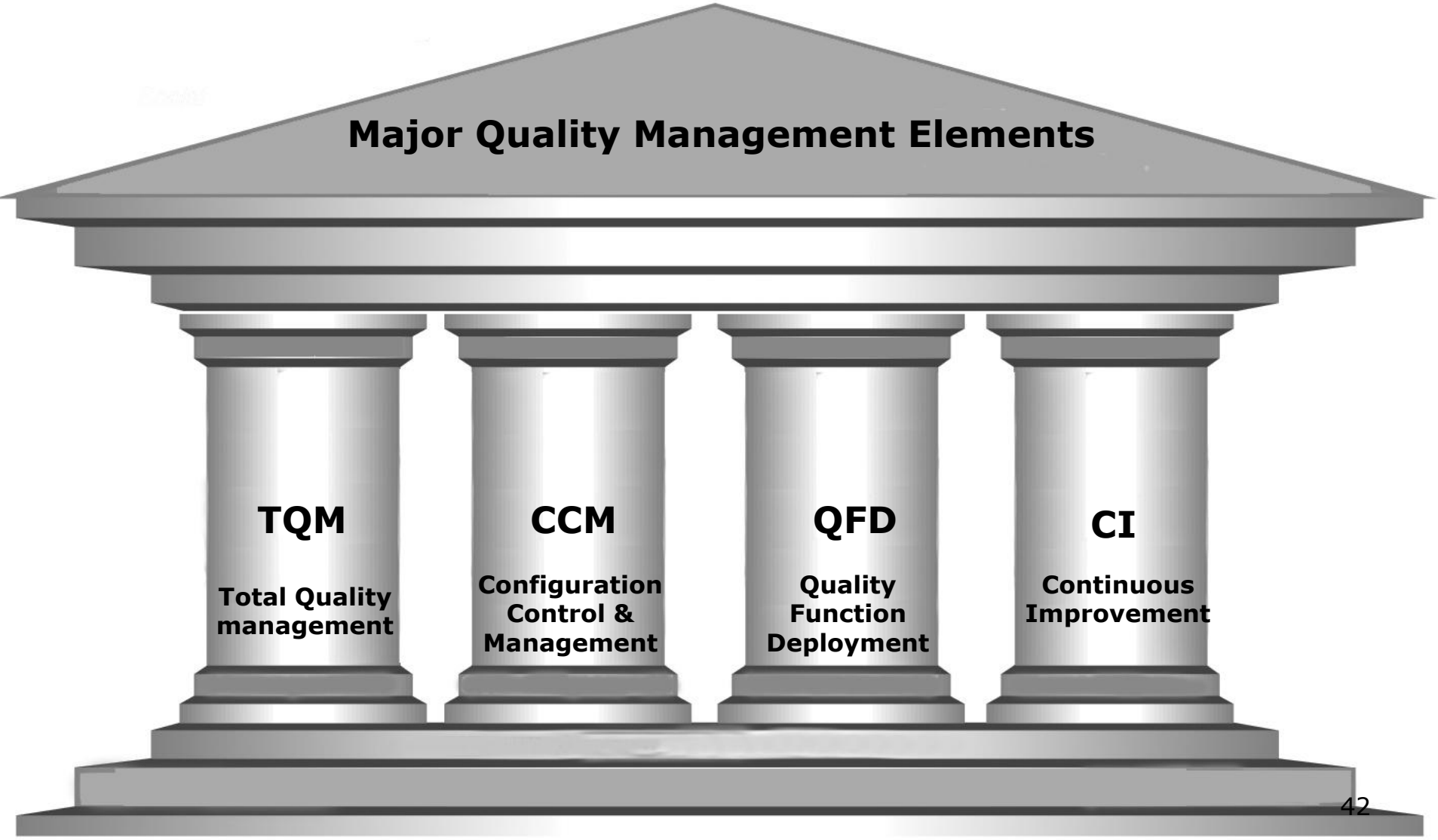
Benefits

- Process improvements
- Financial gain
- Innovation and growth
- Customer satisfaction

QA Process and Benefits (Requirement to Realization)

MEANS	MECHANISM
Quality Control	Use of Tools viz. Cause and effect diagram, Pareto analysis, Histogram, Flow chart, Relationship diagram, Control chart, etc.
Quality Assurance	Use of techniques viz. Statistical process control, Bench mark ing, QFD, FMEA, ISO 9000 and DOE (Control of noise factors and design based on response measurement)
Total Quality Management	Adoption of Industrial engineering approach, *KAIZEN* (continuous improvement), operational research & Managerial accuracy and beyond conformity to standard
Lean Sigma	Use of techniques viz. JIT, Total productive maintenance, Business process re-engineering, Manufacturing resource planning, Statistical measurements (Parametric and tolerance), DMAIC (Define, Measure, Analyze, Improve and Control) approach and Employee culture
Six Sigma	Statistical processes, Elimination of waste, Emphasis on process improvement and Digitization tools

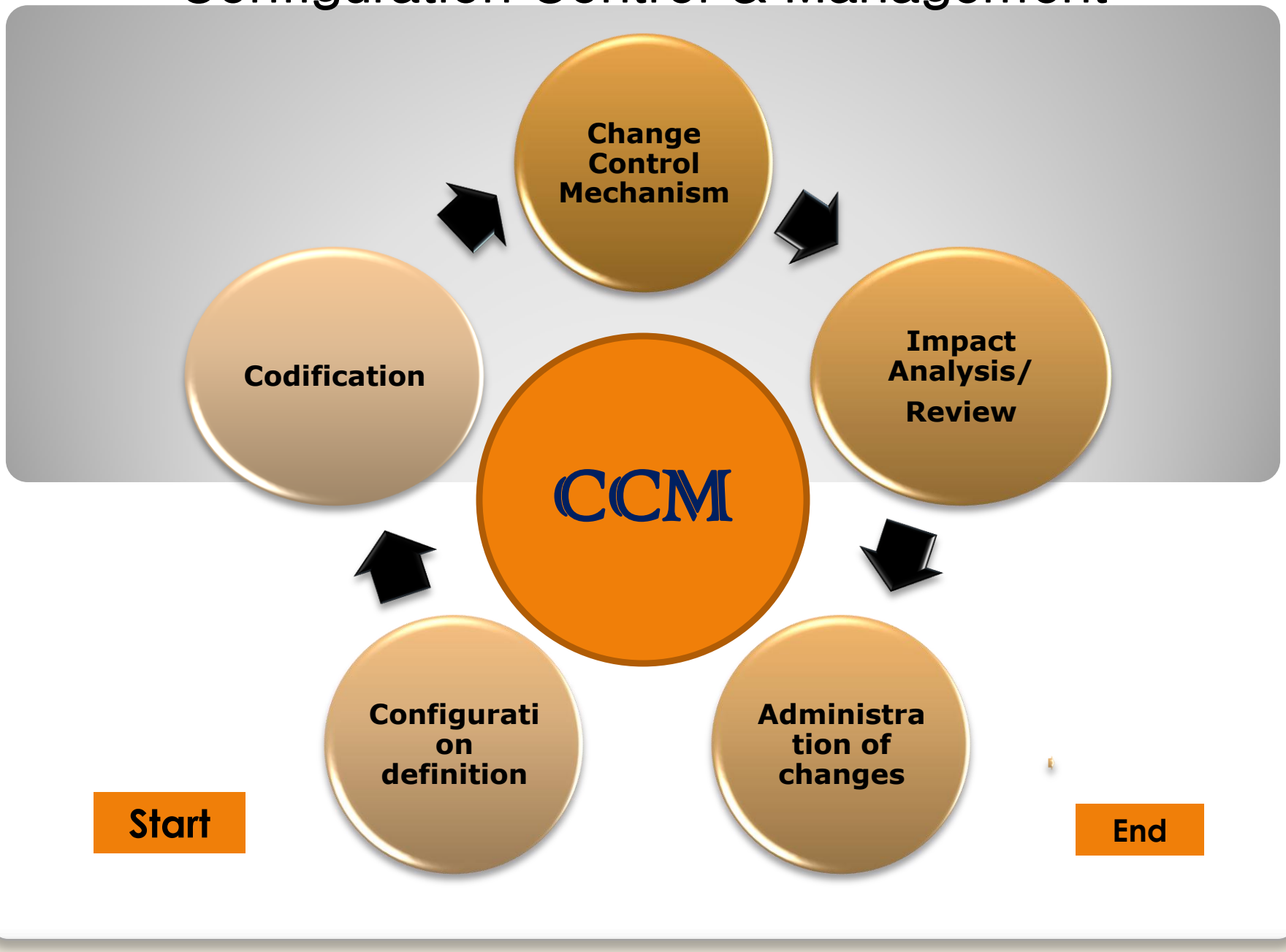
Evolution of QA


Major Quality Management Elements
TQM
Total Quality management
CCM
Configuration Control & Management
QFD
Quality Function Deployment
CI
Continuous Improvement

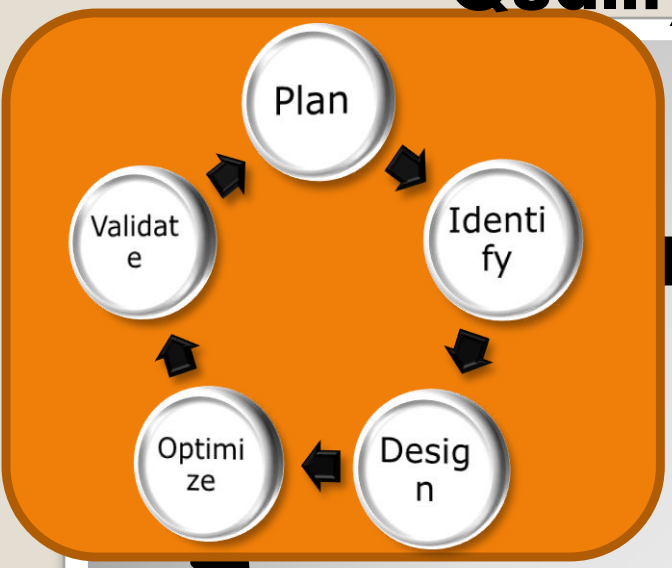
- Use of Concurrent Engineering
- Integrated product & process design
- Formulation of Knowledge based systems
- Virtual Manufacturing
- Involvement of all sections of employees for quality
- Synthetic environment (Modeling & Simulation)
- Extensive standardization of parts / components, materials for wider range of applications-use of COTS.
- Use of validated analysis for demonstration

Principles of TQM

Configuration Control & Management



Quality Function Deployment



Gap Analysis & Corrections / Concession

- User Interactions
- Operational Test pilots as part of the development
- User as stake holder in the programme (PMT)

User defined require-ments

QFD

Voice of Customers (RFAs)

Integrated Logistics Support (ILSS)

- Integrated maintenance Programme
- Simulation Tools for diagnostics & Training
- Optimized Spare Parts management
- Improvised TTGEs
- E-documentations & Records

Start

Continuous Improvement

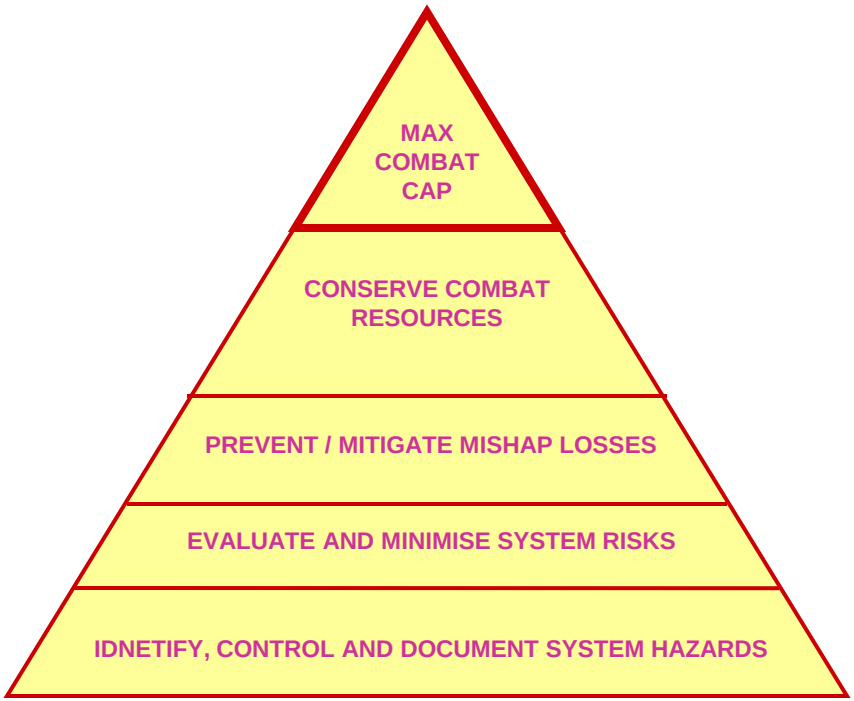
Conventional	***Failure Reporting And Corrective Action System (FRACAS)***
Reactive	Proactive
Qualitative	Quantitative(Measurable)
Logically determined	Analytically determined
Quick - fix solution	Traces to root cause and fixes
Helps to get over and remain	Helps to sustain continuously

System Safety

System Safety Assessment

System Safety Assessment is a systematic comprehensive evaluation of the implemented system functions to show that relevant safety requirements are met

SYSTEM SAFETY GOALS



Why System Safety?

- To obviate a Mishap.
- To undo an inherent hazard potential
- To contain a risk element within acceptable level

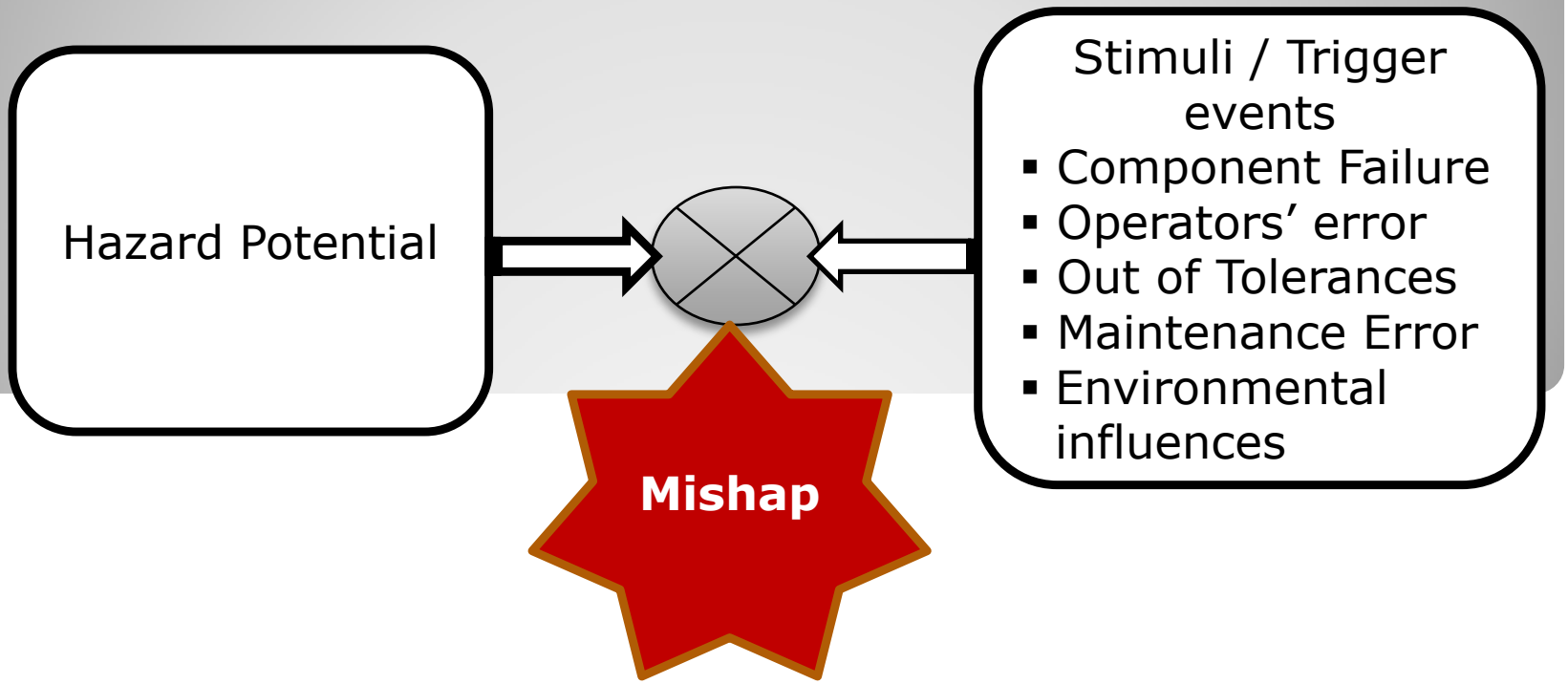
DEFINITIONS

Hazard:
An existing or potential condition that can result in a mishap. In other words, it is a condition that is a prerequisite to mishap.

Mishap:
An unplanned event or series of events resulting in death, injury, occupational illness or damage to or loss of equipment or property or damage to environment.

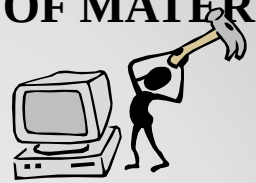
Risk:
An expression as the possibility of mishap in terms of hazard severity and hazard probability.

Mishap


Hazard Potential
Stimuli / Trigger events
Component Failure
Operators' error
Out of Tolerances
Maintenance Error
Environmental influences
Mishap

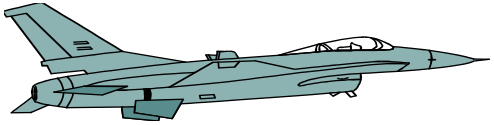
SOURCES OF HAZARDS

- HAZARD CHARECTERISTICS OF MATERIALS & PARTS

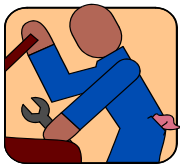


- MALFUNCTION OF EQUIPMENT

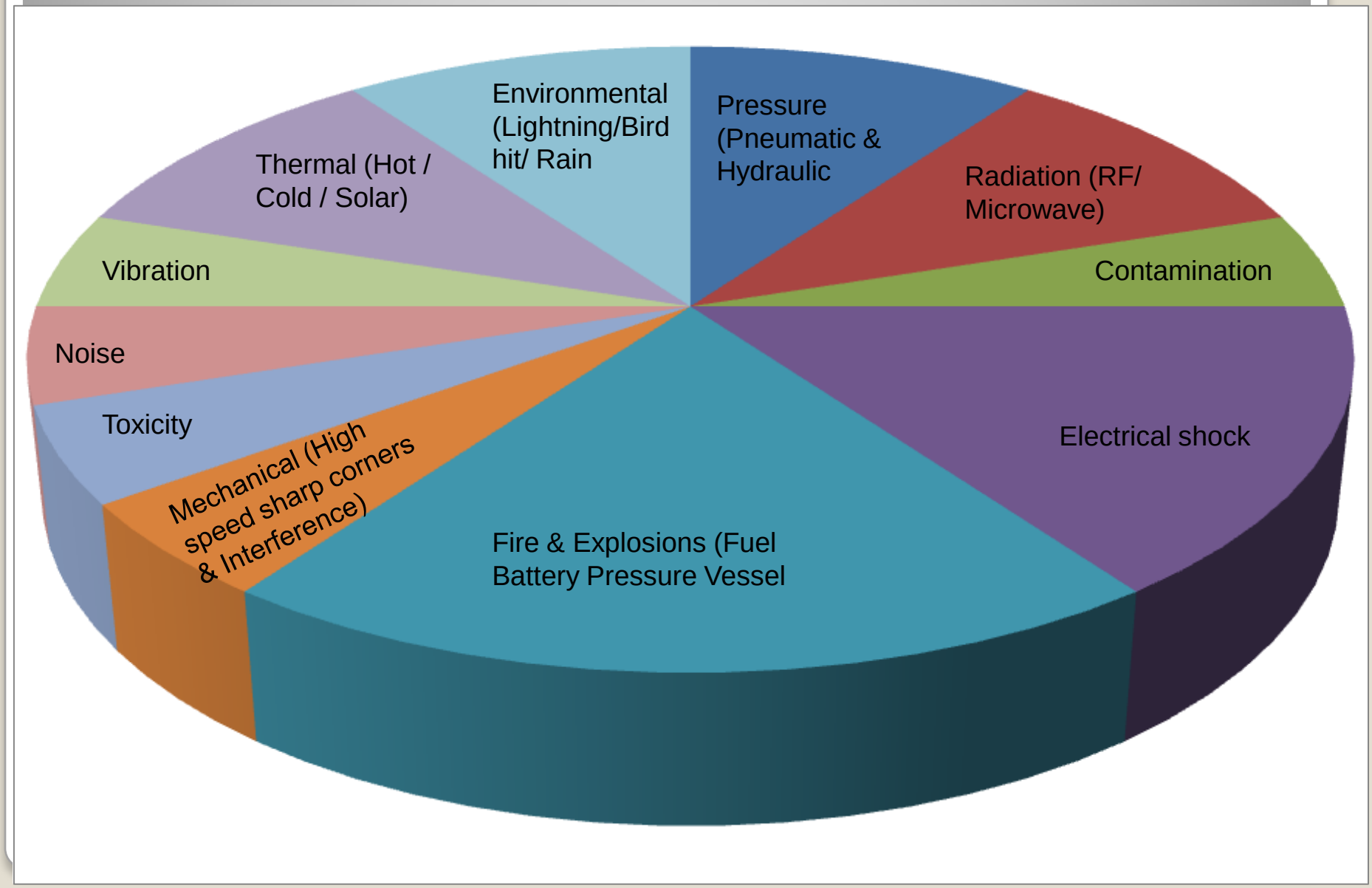
- ADVERSE ENVIRONMENTAL CONDITION



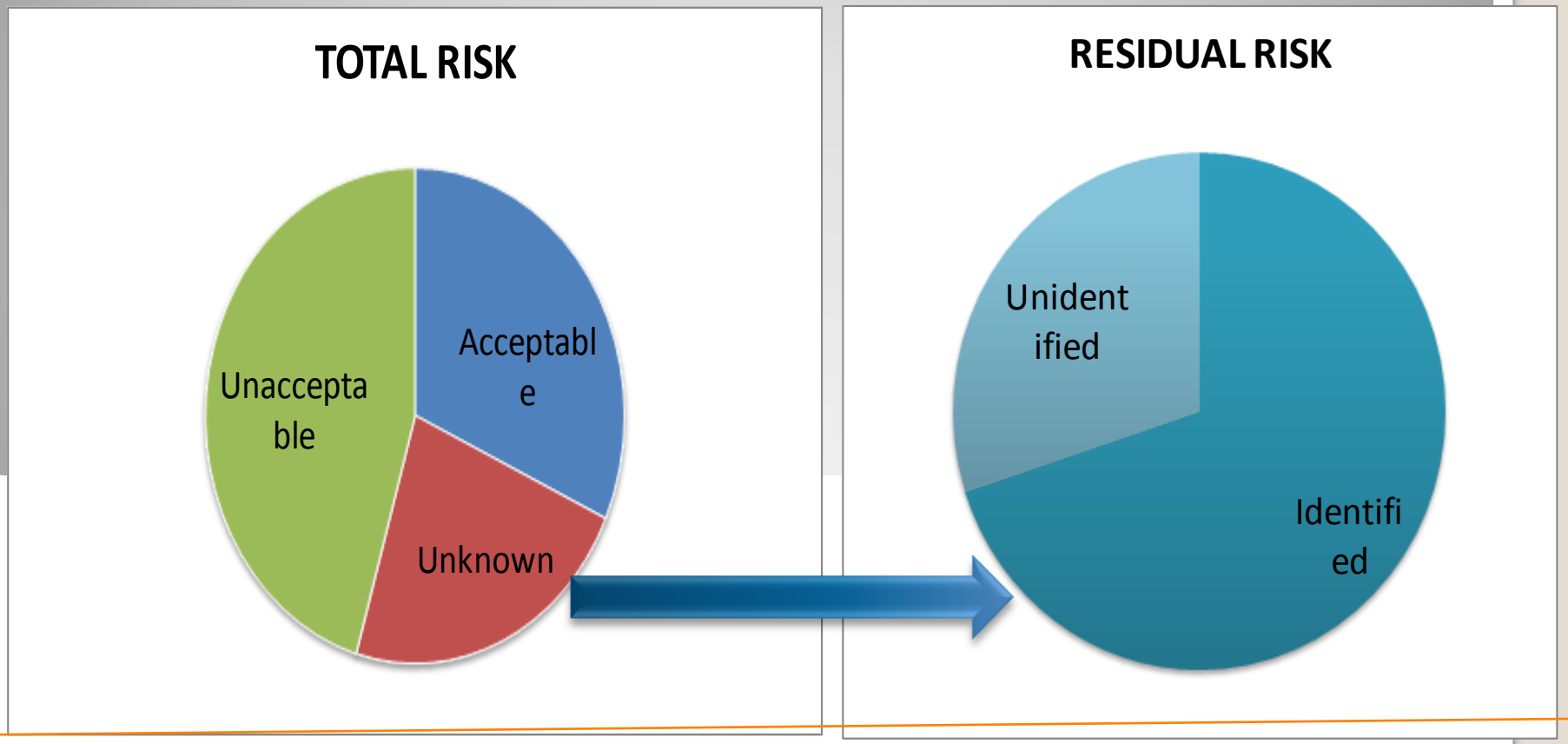
- OPERATORS ERROR



Hazards Spectrum



Risk Spectrum



Genesis behind System Safety Assessment is

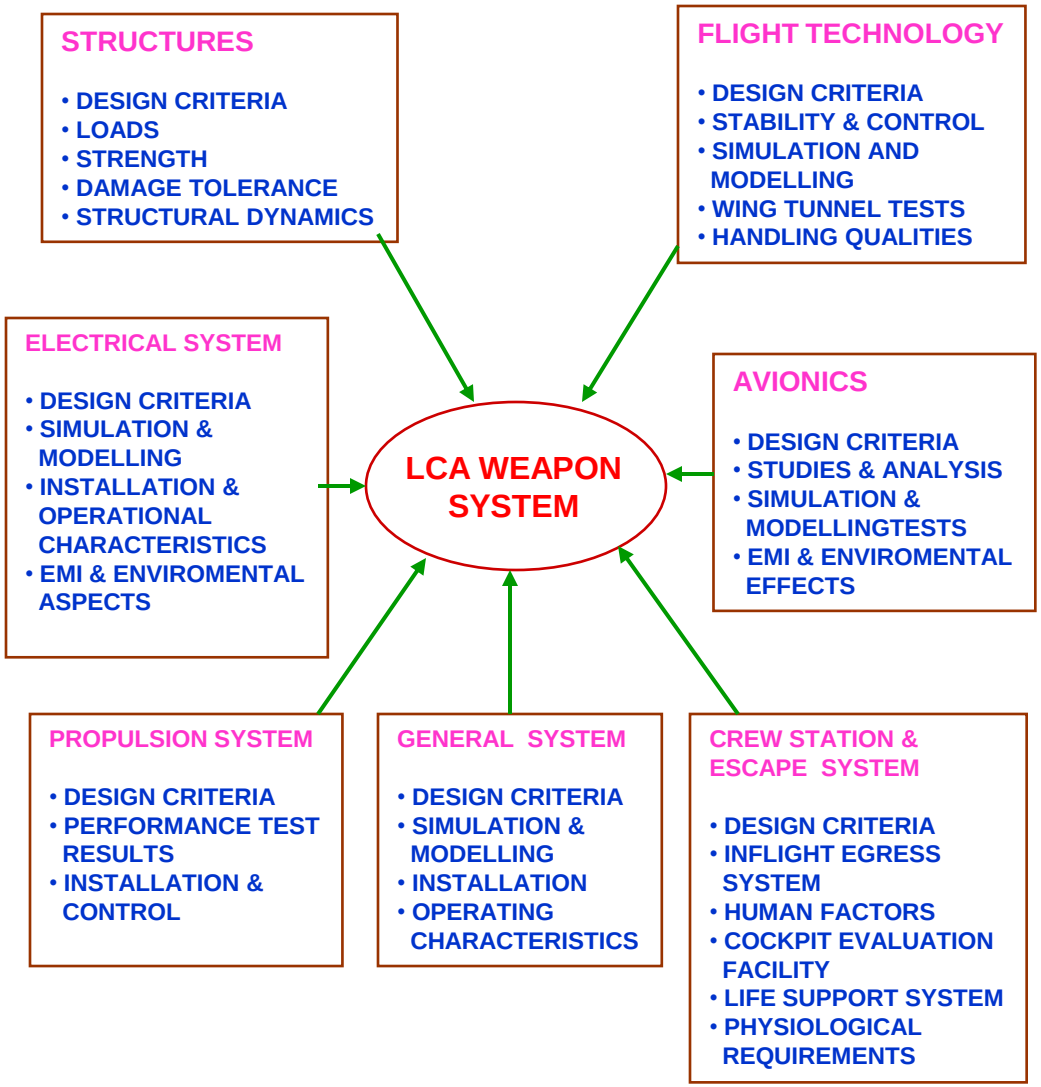
- **To make unidentified Risk as near Zero**
- **In other words, make Residual Risk= Acceptable Risk**

System Safety Analysis:

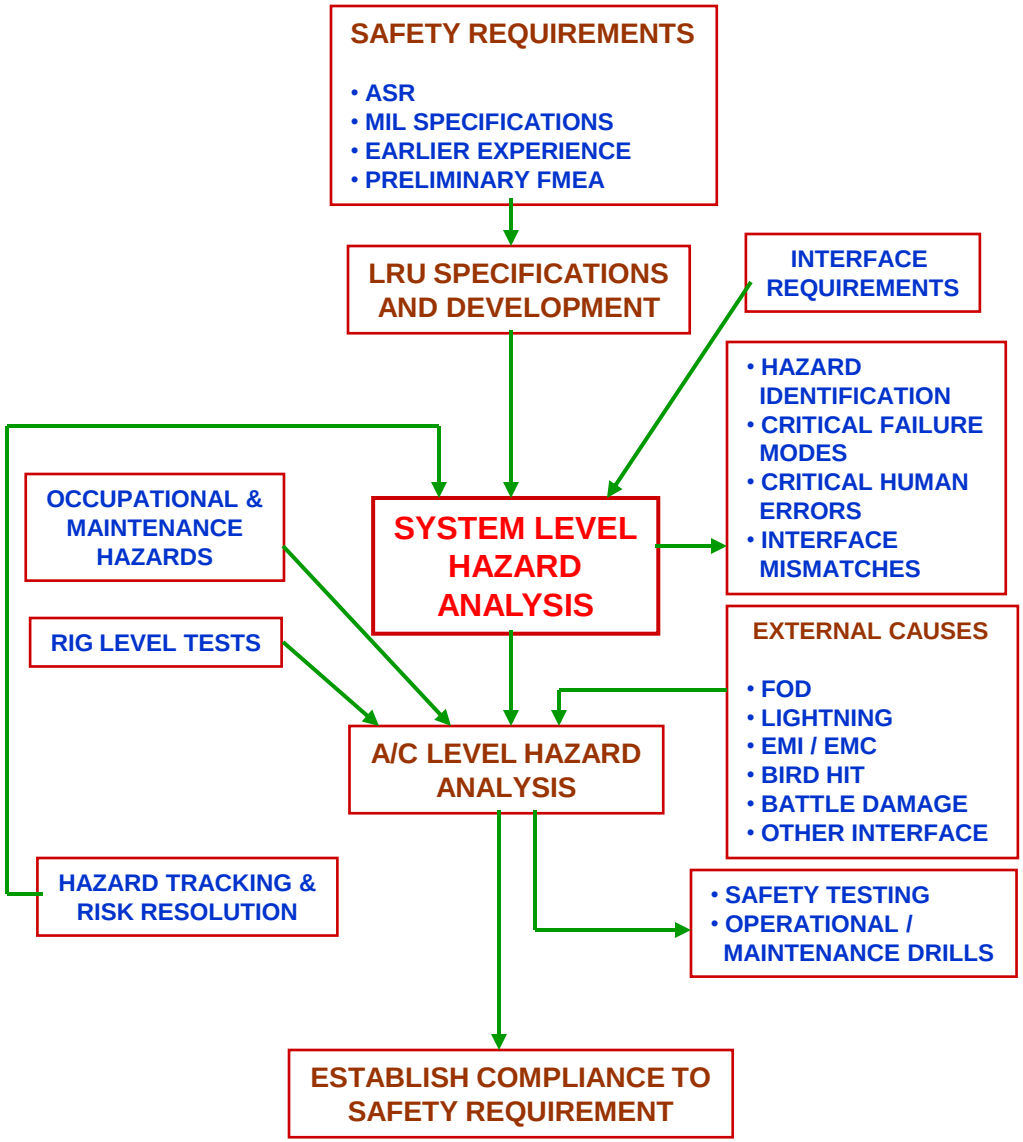
- **It is the a basic tool of the system safety**

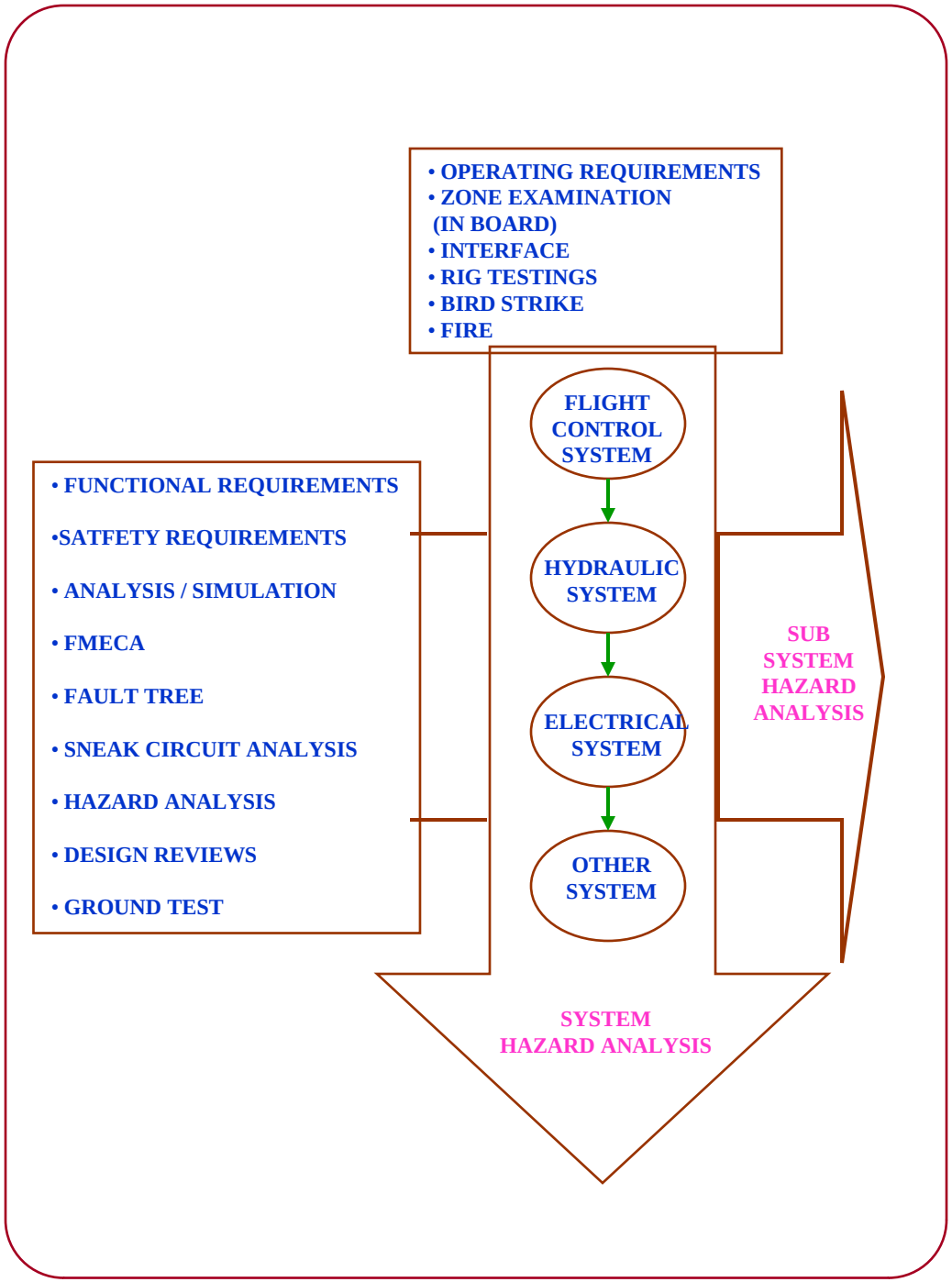
  - To identify the hazards that do exists in a specific system.
  - To determine the causes, effects and interrelationships with inherent hazards potentials.
  - To identify what elements of the system design needs preventive or corrective features.
  - To identify any special tests that should be conducted to verify safety features.

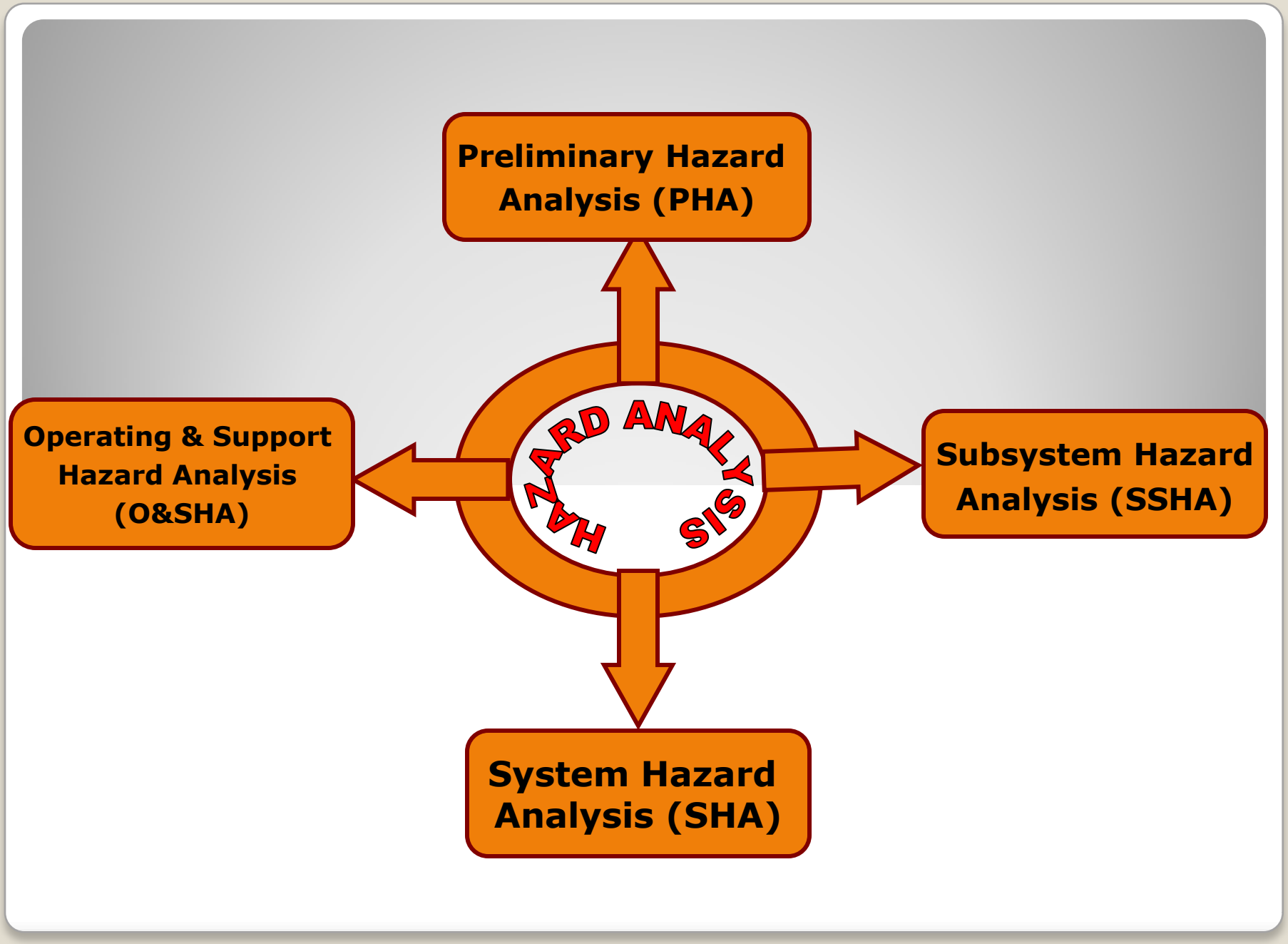
SAFETY EVALUATION DISCIPLINES



AIRCRAFT SYSTEM SAFETY PROCEDURE




• OPERATING REQUIREMENTS
• ZONE EXAMINATION
(IN BOARD)
• INTERFACE
• RIG TESTINGS
• BIRD STRIKE
• FIRE
• FUNCTIONAL REQUIREMENTS
•SATFETY REQUIREMENTS
• ANALYSIS / SIMULATION
• FMECA
• FAULT TREE
• SNEAK CIRCUIT ANALYSIS
• HAZARD ANALYSIS
• DESIGN REVIEWS
• GROUND TEST
FLIGHT CONTROL SYSTEM
HYDRAULIC SYSTEM
ELECTRICAL SYSTEM
OTHER SYSTEM
SUB SYSTEM HAZARD ANALYSIS
SYSTEM HAZARD ANALYSIS


Preliminary Hazard Analysis (PHA)
Operating & Support Hazard Analysis (O&SHA)
HAZARD ANALYSIS
Subsystem Hazard Analysis (SSHA)
System Hazard Analysis (SHA)

Types of Hazard Analysis

MIL 882 - identifies four types of hazard analyses

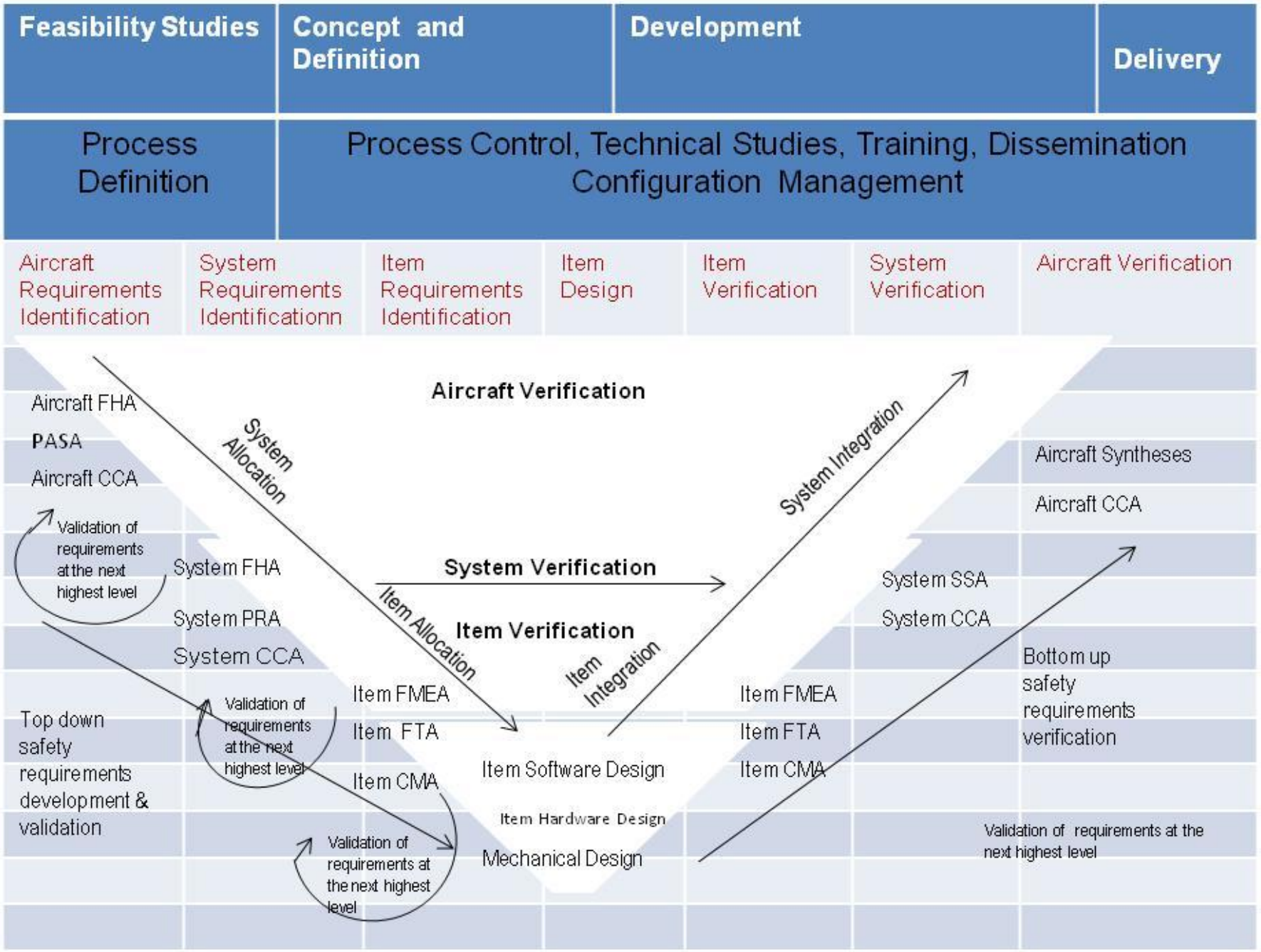
Types of Hazard Analyses	Description
Preliminary Hazard Analysis (PHA)	It is conducted to identify the hazards of various system concepts being considered to satisfy a mission need by using the best information available.
Subsystem Hazard Analysis (SSHA)	The SSHA is conducted to identify the hazards associated with the components of subsystems and interfaces between components of subsystem. Normally SSHA should be conducted during demonstration and validation phase.
System Hazard Analysis (SHA)	The SHA is conducted to determine the hazards associated with interfaces. Normally, it is conducted during start of full-scale development phase.
Operating and support Hazard analysis (O&SHA)	The O&SHA is performed to identify the hazards associated with operating and supporting the system.

DEFINITION OF QUALITATIVE/QUANTITATIVE LEVELS OF HAZARD OCCURANCE

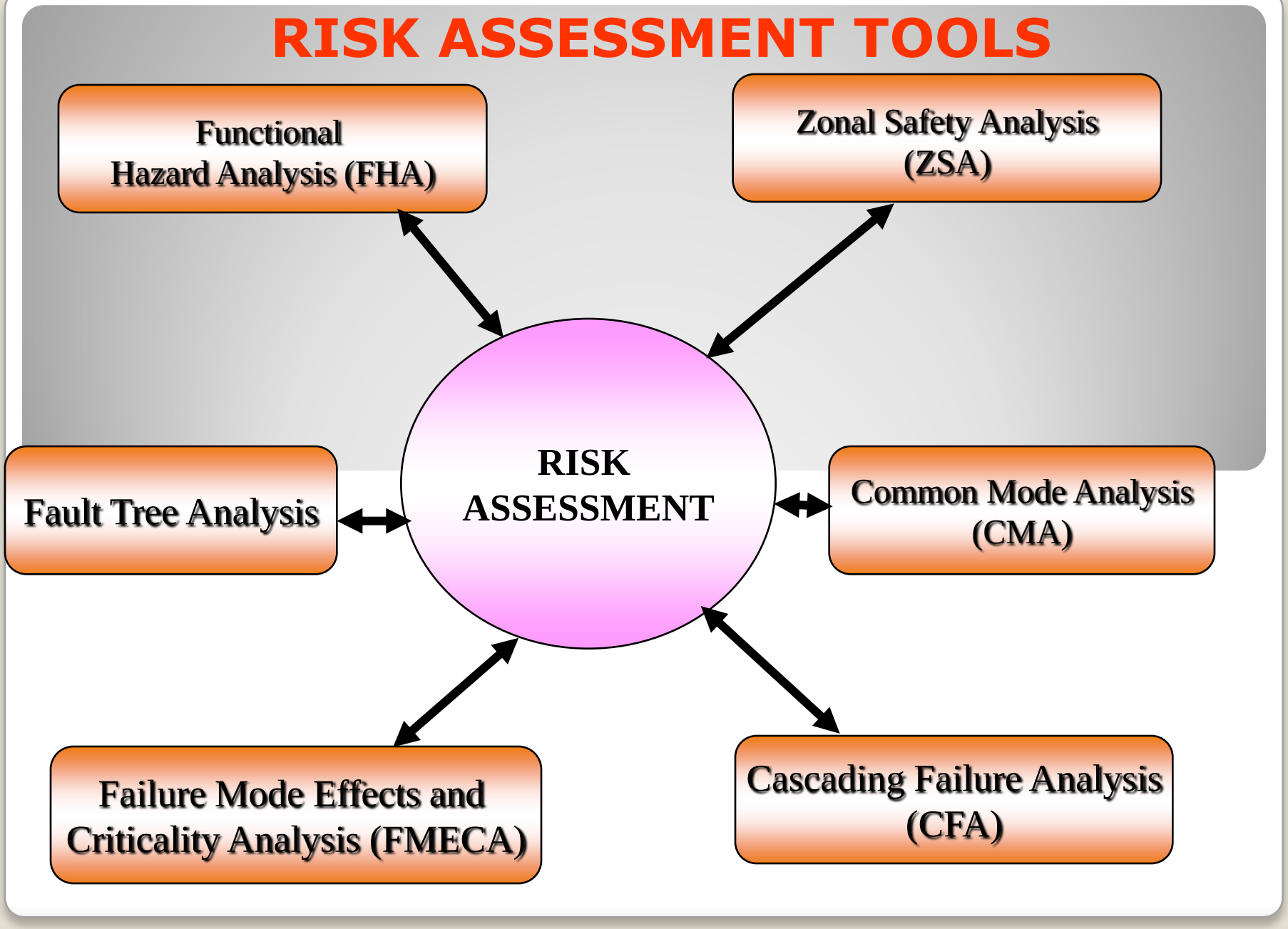
Category	Qualitative Level	Quantitative Level	Mishap Definition
Frequent	A	$> 10^{-1}$	Likely to occur freuently
Probable	B	$10^{-1} – 10^{-2}$	Will occur several times in life of an item
Occasional	C	$10^{-2} – 10^{-3}$	Likely to occur sometime in life of an item
Remote	D	$10^{-3} – 10^{-6}$	Unlikely, but possible, to occur in life of an item
Improbable	E	$< 10^{-6}$	So unlikely, it can be assumed occurrence may not be experienced

DEFINITION OF HAZARD SEVERITY CATEGORIES

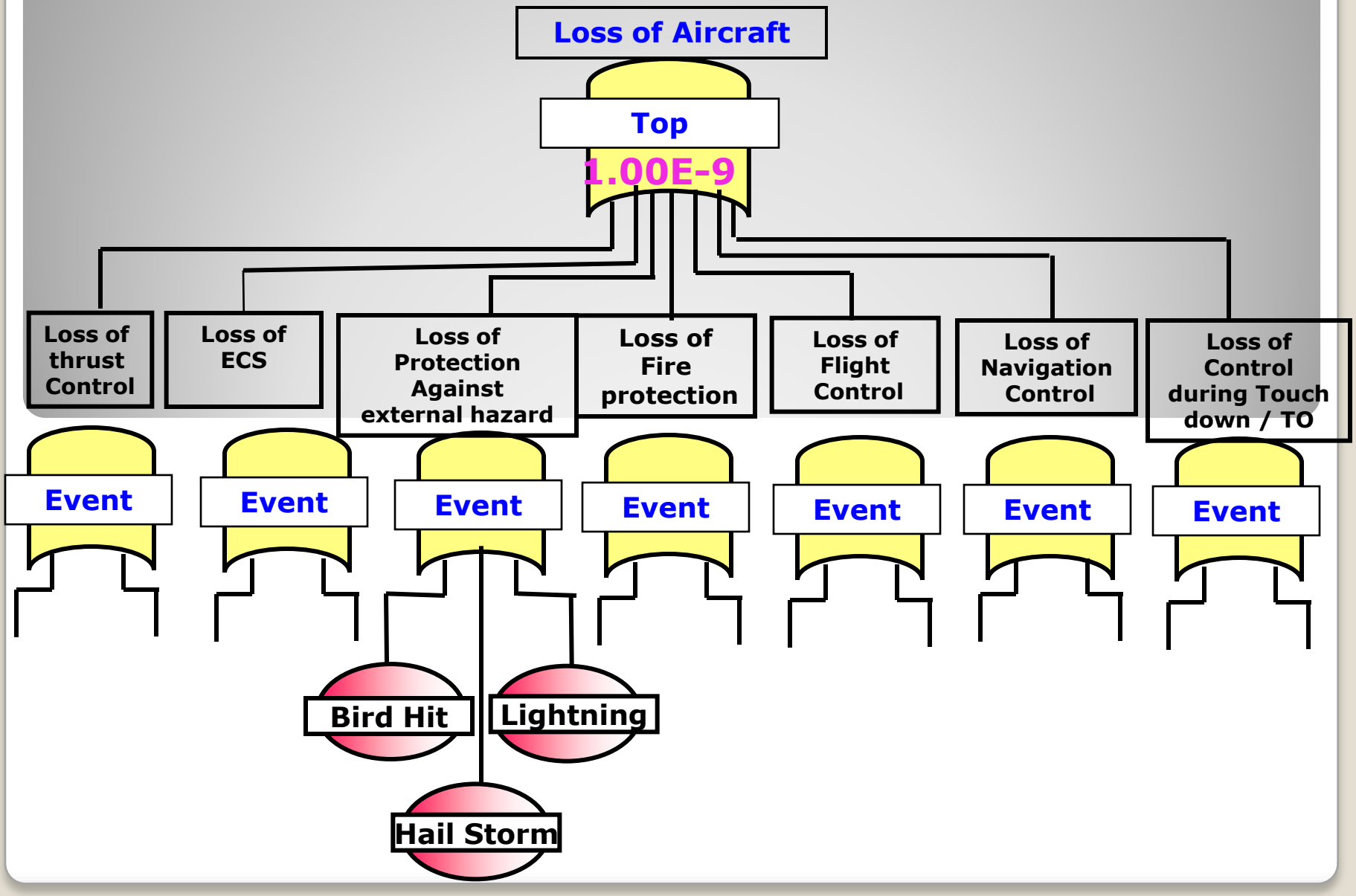
Description	Category	Mishap Definition
Catastrophic	I	Death or System Loss
Critical	II	Sever injury, severe occupational illness, or major system damage
Marginal	III	Minor injury, minor occupational illness, or minor system damage
Negligible	IV	Less than minor injury, occupational illness, or system damage


Feasibility Studies
Concept and Definition
Development
Delivery
Process Definition
Process Control, Technical Studies, Training, Dissemination
Configuration Management
Aircraft Requirements Identification
System Requirements Identificationn
Item Requirements Identification
Item Design
Item Verification
System Verification
Aircraft Verification
Aircraft Verification
Aircraft FHA
PASA
Aircraft CCA
System Allocation
System Integration
Aircraft Syntheses
Aircraft CCA
Validation of requirements at the next highest level
System FHA
System Verification
System SSA
System PRA
System CCA
Item Allocation
Item Verification
Item Integration
System CCA
Item FMEA
Item FMEA
Bottom up safety requirements verification
Validation of requirements at the next highest level
Top down safety requirements development & validation
Item FTA
Item FTA
Item CMA
Item Software Design
Item CMA
Item Hardware Design
Validation of requirements at the next highest level
Mechanical Design
Validation of requirements at the next highest level

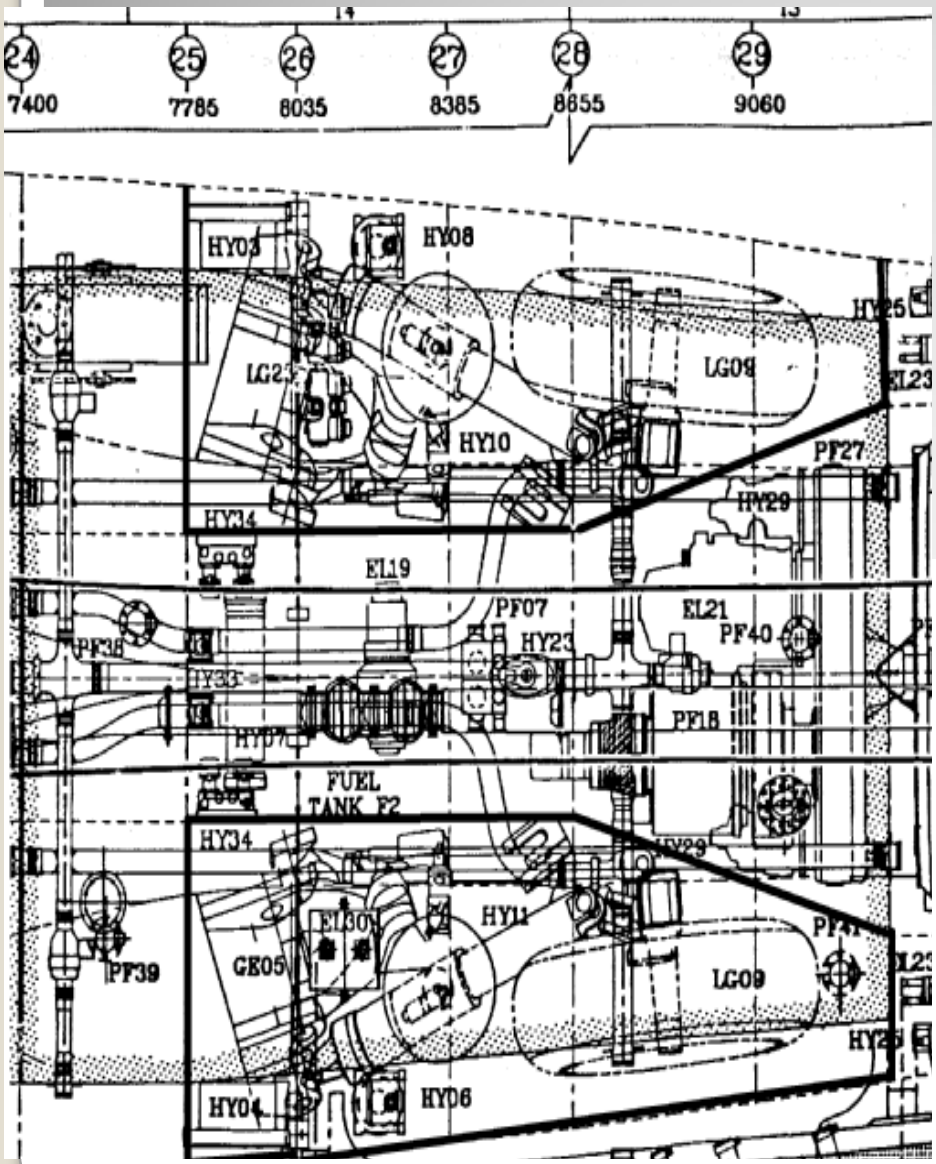
RISK ASSESSMENT TOOLS



Particular Risk Analysis by FTA



Zonal Safety Analysis



Normal Operating Condition

Neighbouring

- LRUs
- **Tanks/ Reservoirs**
- **Rotating Assemblies**
- **Pipelines**
- **Limitations /wavier for design**

Abnormal Operating Condition

Effect on identified **LRU & A/C** in a zone, Availability of failure indication

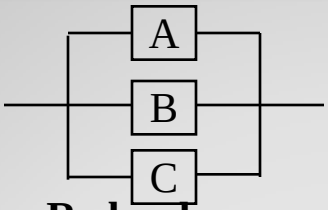
Failures of neighboring LRUs

Principles of Zonal Safety

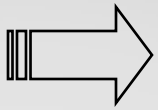
Though equipment location is dictated by its operation and interface, nevertheless evaluated for

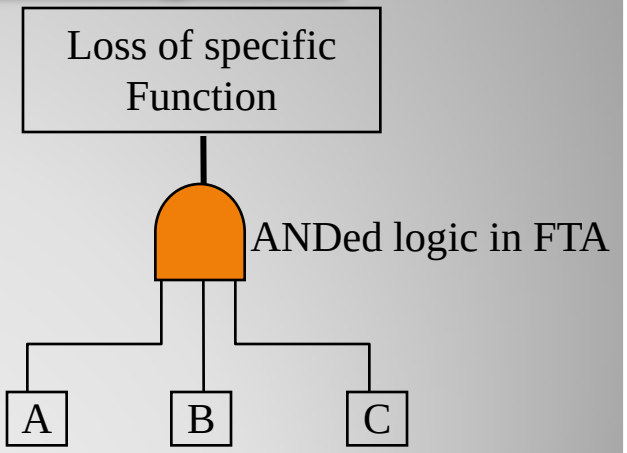
- Safety requirement by virtue of co-located equipments, not being congenial for trigger events
- Isolation for redundant systems
- Consideration for EM interference
- Inspectability, accessibility and replaceability

Common Mode Analysis



Redundancy





Human error– Maintenance, Inspection

Thermal effect

Leak - combustible substances/hot air

Power supply

Installation

Ground Path

Sharing of Connectors

Common links – structural /electrical

FOD

EMI /Lightning

Transients

Cable bundling

Common Mode

Cascading Failure Analysis

Relational Matrix

FAILURE OF SYSTEMS	System ←No.	SYSTEMS	FAILURE EFFECT ON RESPECTIVE SYSTEM												
			1	2	3	4	5	6	7	8	9	10	11	12	13	14
	1	*Engine (ENG)*	1-1	1-2	1-3	1-4	1-5	1-6	1-7	1-8	1-9	1-10	1-11	Nil	Nil	1-14
	2	*Hydraulics (HYD)*	Nil	2-2	2-3	2-4	2-5	Nil	Nil	Nil	2-9	2-10	2-11	Nil	2-13	Nil
	3	*Electrical (ELEC)*	3-1	3-2	3-3	3-4	3-5	3-6	Nil	3-8	3-9	3-10	3-11	3-12	3-13	3-14
	4	*Integrated Flight Control System (IFCS)*	4-1	Nil	Nil	4-4	Nil	Nil	Nil	4-8	Nil	Nil	Nil	Nil	Nil	Nil
	5	*Fuel*	5-1	5-2	5-3	5-4	5-5	Nil	5-7	Nil	Nil	Nil	Nil	Nil	Nil	Nil
	6	*Environmental Control System (ECS)*	6-1	Nil	Nil	6-4	6-5	6-6	Nil	6-8	Nil	Nil	Nil	Nil	6-13	Nil
	7	*Secondary Power System (SPS)*	7-1	7-2	7-3	7-4	7-5	7-6	7-7	7-8	7-9	7-10	7-11	Nil	7-13	Nil
	8		8-1	8-2	8-3	8-4	8-5	8-6	8-7	8-8	8-9	Nil	8-11	Nil	Nil	Nil
	9		Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	9-9	Nil	Nil	Nil	9-13	Nil
	10		Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	10-10	Nil	Nil	Nil	Nil
	11		Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	11-11	Nil	Nil	Nil
	12		Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	12-12	12-13	Nil
	13		13-1	Nil	Nil	13-4	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	13-13	Nil
	14		Nil	Nil	Nil	14-4	Nil	Nil	Nil	14-8	Nil	Nil	Nil	Nil	Nil	14-14

- **Diagonal Elements**
- **Relationship x-y**
- **'NIL' assignment to both column and row**
- **Development of each row in the respective Cascading Failure Effect (CFE) matrix.**

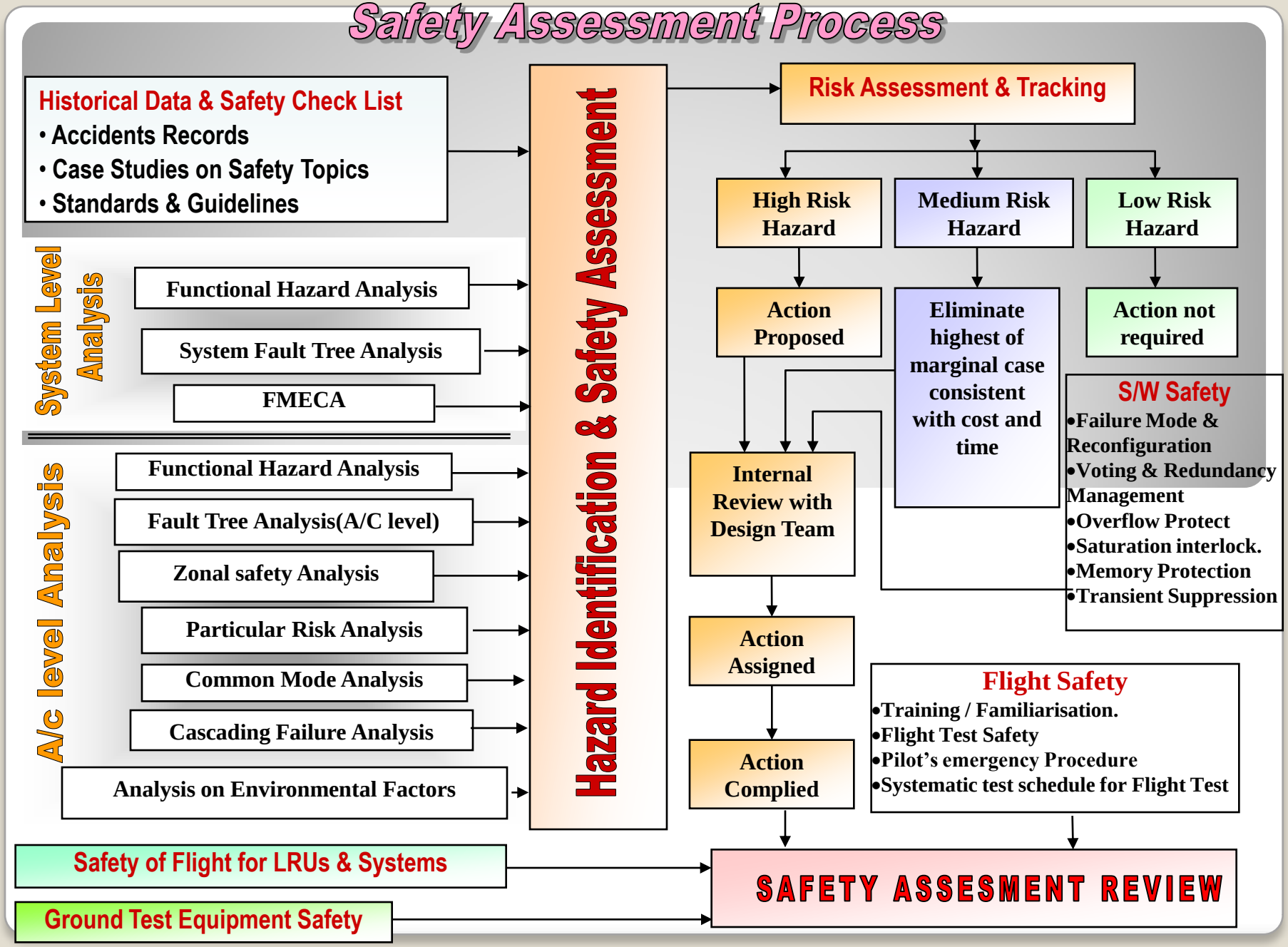
Probabilistic Risk Assessment
As per MIL-STD-882 C

[BASED ON *SEVERITY* CLASSIFICATION & FREQUENCY OF OCCURRENCE]

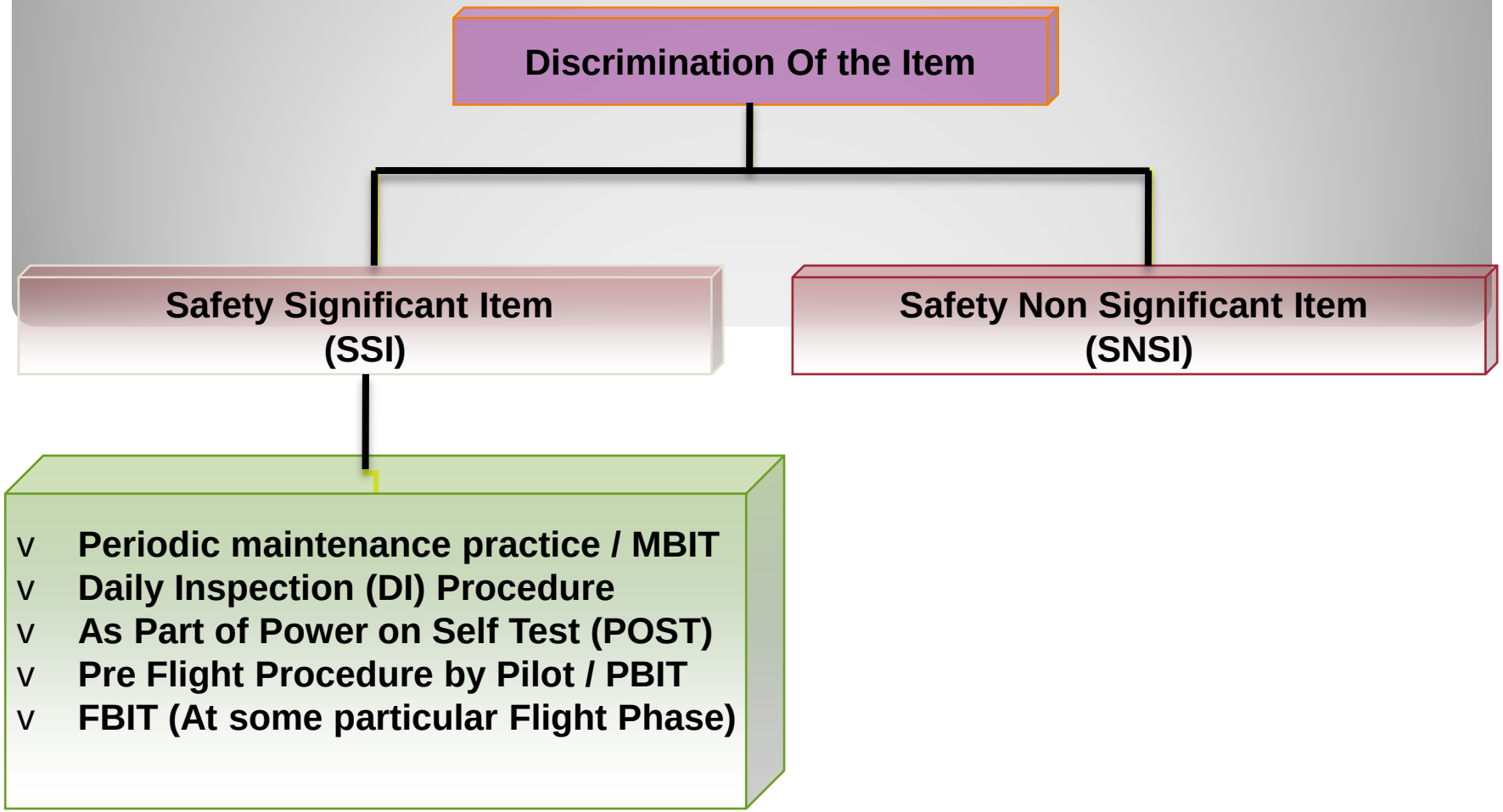
Frequency \ Hz Cat	I	II	III	IV
Frequent> 10^{-1}	1	3	7	13
Probable 10^{-1} - 10^{-2}	2	5	9	16
Occasional 10^{-2} X 10^{-3}	4	6	11	18
Remote 10^{-3} X 10^{-6}	8	10	14	19
Improbable < 10^{-6}	12	15	17	20

Hazard Risk Index	Suggested Criteria
1 -5	Unacceptable
6 -9	Undesirable
10 -17	Acceptable with review
18 -20	Acceptable without review

Safety Assessment Process



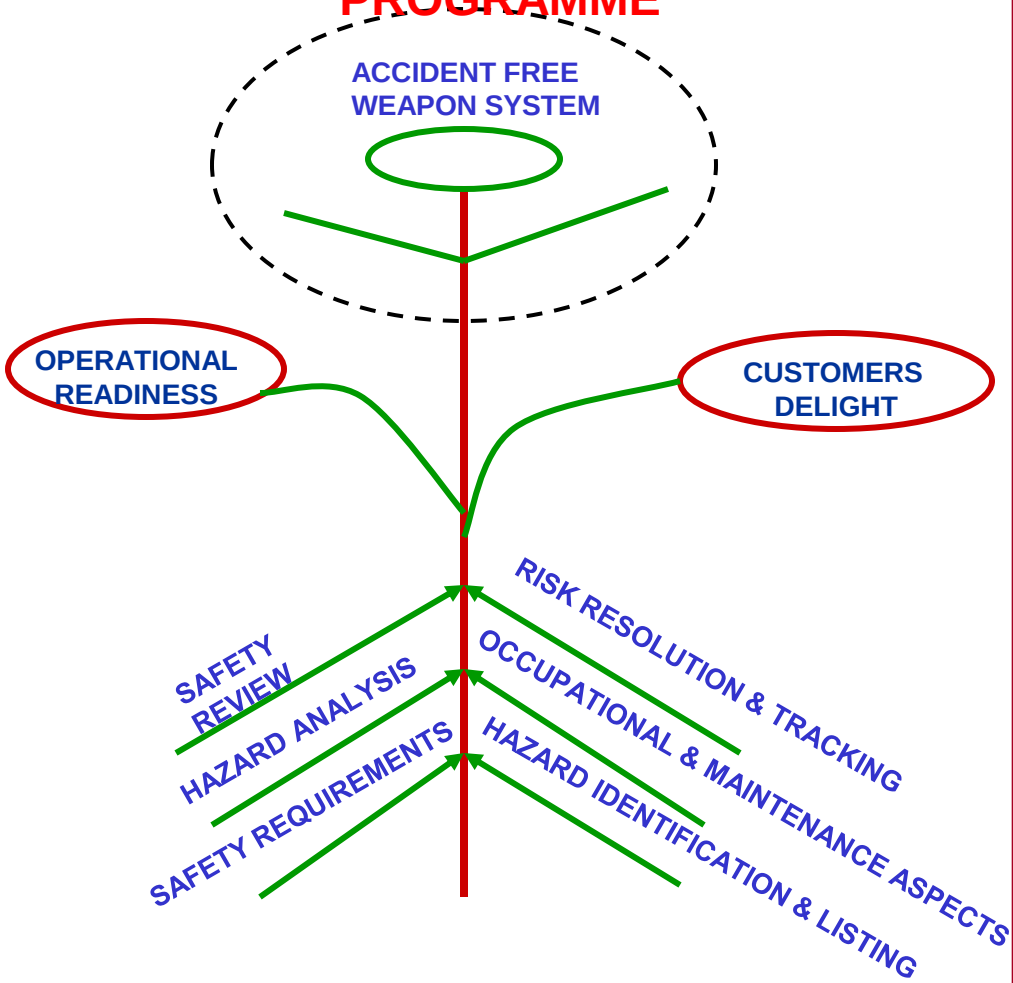
Discrimination of the Item



REVIEW MECHANISM

- PDR / CDR / QR for design adequacy
- Rig level assessment (FMET)
- TRR / Safety Review / FRRB for integration level
- Maintenance safety review
- Pilot Emergency Procedure review
- Telemetry safety / Flight Instructions /Data review and analysis

FRUITS OF SYSTEM SAFETY PROGRAMME



Reliability, Maintainability, Quality, Standards

Standards

MIL-HDBK-217F	:	Reliability Prediction Of Electronic Equipment
MIL-HDBK-338	:	Electronic Reliability Design Handbook
MIL-HDBK-764	:	System Safety Engineering Design Guide For Army Materiel
MIL-HDBK-781A	:	Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production
MIL-STD-785-Rev B	:	Reliability Program For Systems And Equipment,
MIL-STD-1629-RevA	:	Procedures For Performing A Failure Mode, Effects and Criticality Analysis
MIL-STD-2155	:	Failure Reporting, Analysis And Corrective Action System Maintainability
MIL-STD-2165	:	Testability Program For Electronic Systems And Equipment,
MIL-STD-2173	:	Reliability-Centered Maintenance Requirements for Naval Aircraft, Weapons Systems and Support Equipment
MIL-HDBK-472	:	Maintainability Prediction
DOD-HDBK-791	:	Maintainability Design Techniques,
MIL-HDBK-2084	:	Handbook For Maintainability Of Avionic And Electronic Systems and Equipment

MIL-STD-1843	:	Reliability-Centered Maintenance for Aircraft, Engines and Equipment.
MIL-STD-2084	:	Maintainability of Avionic & Electronic Systems and Equipment Quality
MIL-HDBK-2164A	:	Environmental Stress Screening Process,
MIL-HDBK-46855	:	Human Engineering Program Process And Procedures
MIL-STD-810	:	Test Method Standard For Environmental Engineering Considerations And Laboratory Tests
MIL-STD-1472D	:	Human Engineering Design Criteria For Military Systems, Equipment And Facilities
MIL-STD-1586	:	Quality Program Requirements For Space And Launch Vehicles

Reference Books:

- Assurance Technologies, Principles and Practices by Dev G.Raheja
- Reliability and Maintainability Engineering by Charles E.Ebeling
- Reliability Engineering Handbook, Vol.1 and 2, by Dimitri Kececioglu

Applicable Standards for SSA

1. MIL-HDBK-764 System Safety Engineering design guide
2. MIL 882 C System Safety Program Requirement
3. DEF Std 00-970 on design and airworthiness requirements for service aircraft.
4. ARP4761 on guidelines and methods for conducting the safety assessment process
5. WL document no. ASCP-800 defining requirements for readiness review for first flight
6. BAe report on System safety Assessment no. AWN/GEN/497/ISSUE/01 dated October 1988

References

1) ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems.
2) ARP4754 Certification Considerations for Highly-Integrated or Complex Aircraft Systems, 996.
3) AC 25.1309-1A System Design and Analysis, Advisory Circular, 1998
4) AMJ 25.1309 System Design and Analysis, Advisory Material Joint, 1994
5) ATA-100 ATA Specification for Manufacturer's Technical Data.
6) DO-178B Software Considerations in Airborne Systems and Equipment Certification.
7) DO-254 Design Assurance Guidance for Airborne Electronic Hardware.
8) DEF STAN 00-970 Volume 1 Amendment 12: Design and Airworthiness Requirements for Service Aircraft.
9) DEF STAN 00-35 Environmental handbook for Defence Material.
10) DEF STAN 07-55 Environmental Testing of Service Materia
11) BG 3G 100: General Requirements for Equipment for use in Aircraft-Part-2: All Equipment

1) DEF STAN 00-970 Volume 1 Amendment 12: Design and Airworthiness Requirements for Service Aircraft.
2) DEF STAN 00-35 Environmental Handbook for Defence Material.
3) BS 3G 100: General Requirements for Equipment for use in Aircraft – Part 2: All Equipment.
4) DEF STAN 07-55 Environmental Testing of Service Material.

IN SUMMARY

- **Performance effectiveness is one of the key constituent of system engineering.**
- **Assurance technologies are the means to enhance the performance enhancement and also to effect cost effectiveness.**
- **Reliability, Maintainability, Human Factors and System safety are the basic disciplines of Assurance technologies.**
- **There are several techniques to engineering the reliability and the best practices adopted widely across the industries are the one which would fetch the optimal benefits.**
- **Maintainability features are the key to enhance the availability.**

Contd/-

THANK YOU

- ADDITIONAL MATERIAL

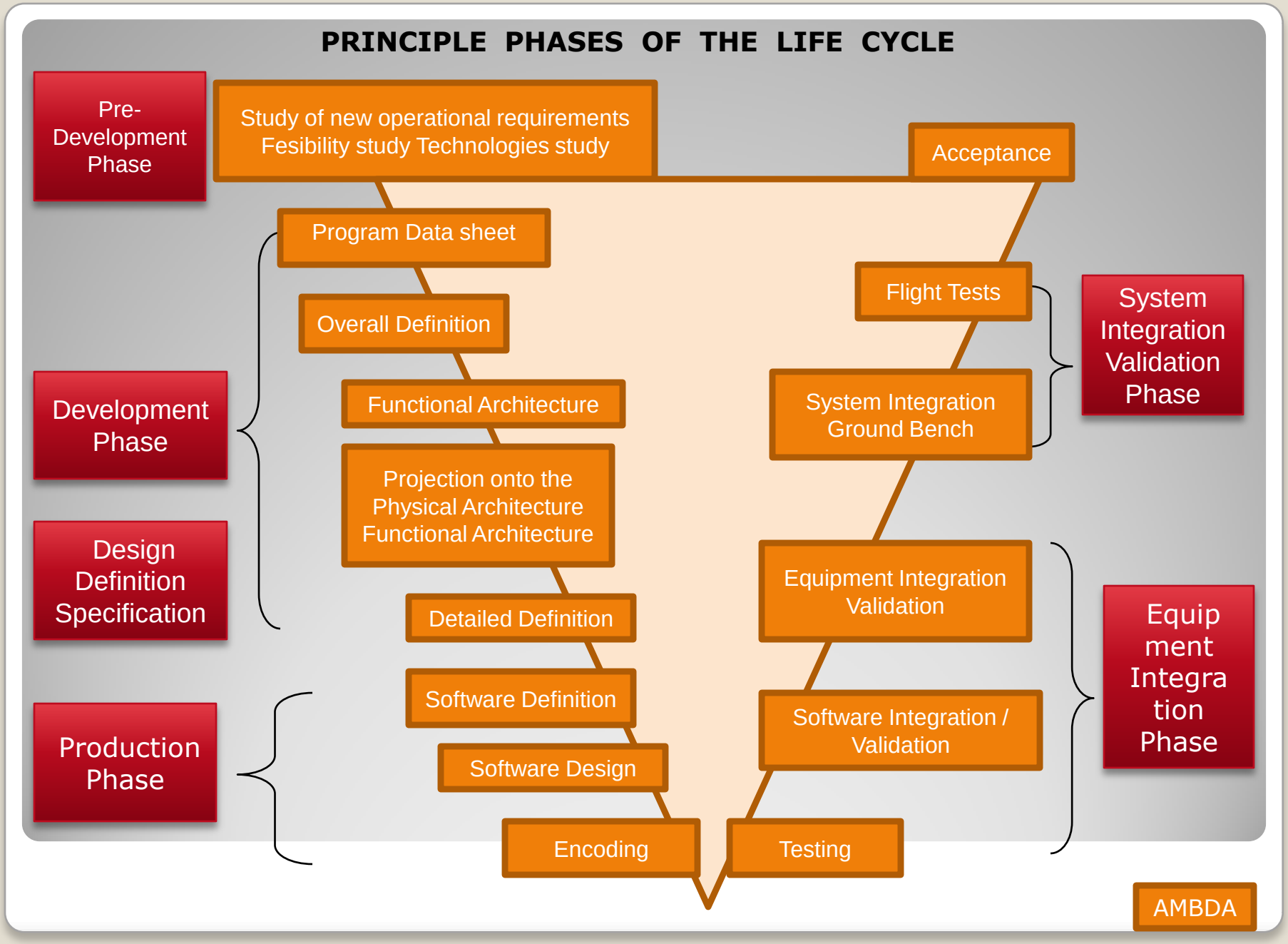
1	Components with history of high defect / failure rates	Very high Above 50/mil.hr	Moderately high upto 50/mil.hr	Low Upto 20/mil.hr.
2	Components which are newly developed and which therefore have uncertain reliability characteristics	Very new	Moderately new	Already matured
3	Components whose function is particularly important to the achievement of the total equipment function – for mission Accomplishment / Safe return	A or B in single failure mode	A or B with double failure C&D single failure	E (No effect)
4	Components the failure of which could cause a safety hazard e.g. Leakage of inflammable fluids, exposition, etc.	Instantaneous safety hazard within 30 secs.	Take 30min. To cause safety hazard	Not very much

CRITERIA FOR VED ANALYSIS

5	Components being used in an environment about which little is known or which is more stringent than that to which the component has previously been subjected	Stringent environment, previously unsubjected to	Stringent environment but previously subjected to	Environment not a criteria
6	Components which involve large repair costs / time	Repair time / cost very higher	Moderate	Negligible
7	Components complexity	Highly complex	Moderately complex	Simple
8	Components which might be subjected to reliability variance resulting from production tolerance	More than 3 value	Value	Negligible

Note: 1. If 3&4 are vital, component is rated as vital
2. If 3&4 are essential, component is rated as essential
3. If any 3 are vital out of 8, then comp. is rated as vital
4. If any 3 are essential out of 8, then comp. is rated as essential

CRITERIA FOR VED ANALYSIS (Contd.)


PRINCIPLE PHASES OF THE LIFE CYCLE
Pre-Development Phase
Study of new operational requirements
Fesibility study Technologies study
Acceptance
Program Data sheet
Flight Tests
System Integration Validation Phase
Overall Definition
Development Phase
Functional Architecture
System Integration Ground Bench
Projection onto the Physical Architecture Functional Architecture
Design Definition Specification
Equipment Integration Validation
Equipment Integration Phase
Detailed Definition
Software Definition
Software Integration / Validation
Production Phase
Software Design
Encoding
Testing
AMBDA

The subsystems covered under this category are emergency backup / standby systems to the main system or purely safety devices. These are generally passive, but called upon to play their role at the time of crisis / emergency. Their failure may lead to hazardous consequences to aircraft and / or air crew.

SAFETY CRITICAL

FLIGHT CRITICAL (FC)

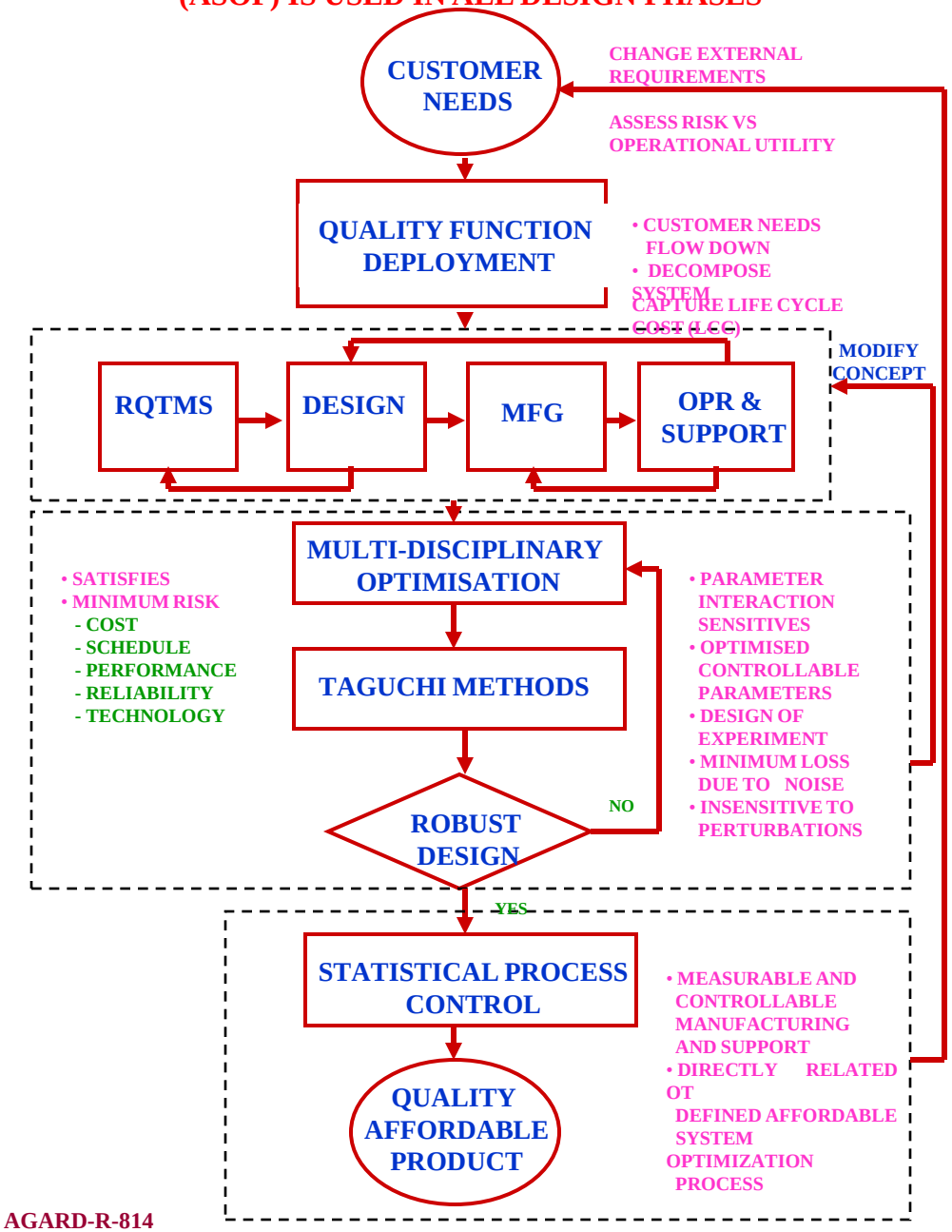
The subsystems covered under this category upon failure during any phase of the flight may endanger the flight safety of the aircraft.

MISSION CRITICAL (MC)

The subsystems under this category upon failure shall result in **'Mission Abort'** situation or mission degradation.

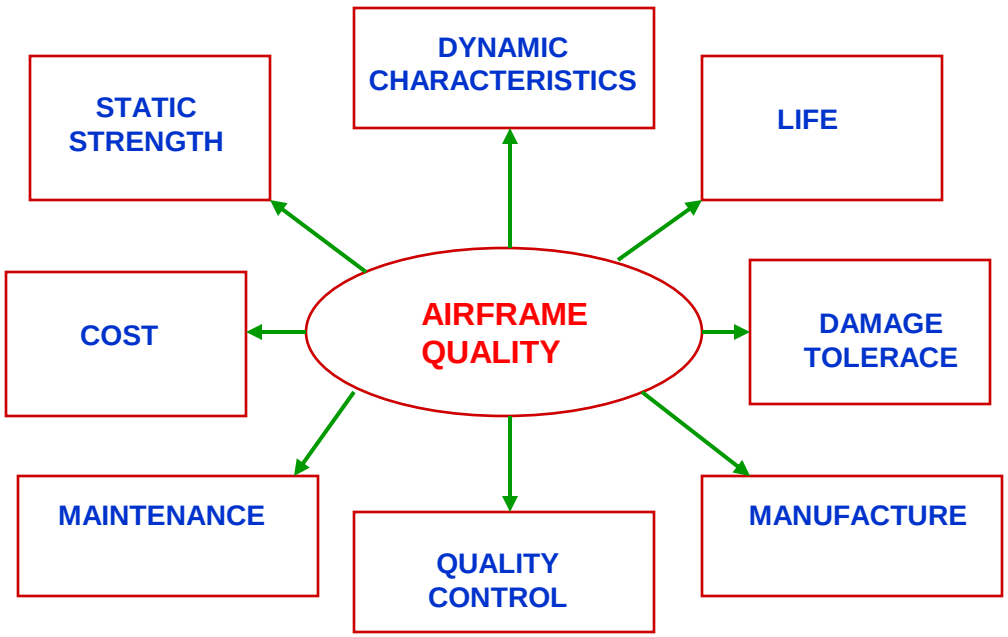
Contd.

THE "AFFORDABLE SYSTEMS OPTIMIZATION PROCESS" (ASOP) IS USED IN ALL DESIGN PHASES



AIRFRAME QUALITY

AIRFRAME PERFORMS AS SPECIFIED DURING THE REQUIRED LIFE TIME WHEN USED AS INTENDED WITH PROPER MAINTAINANCE WITHOUT ANY FAILURE



REFERENCES

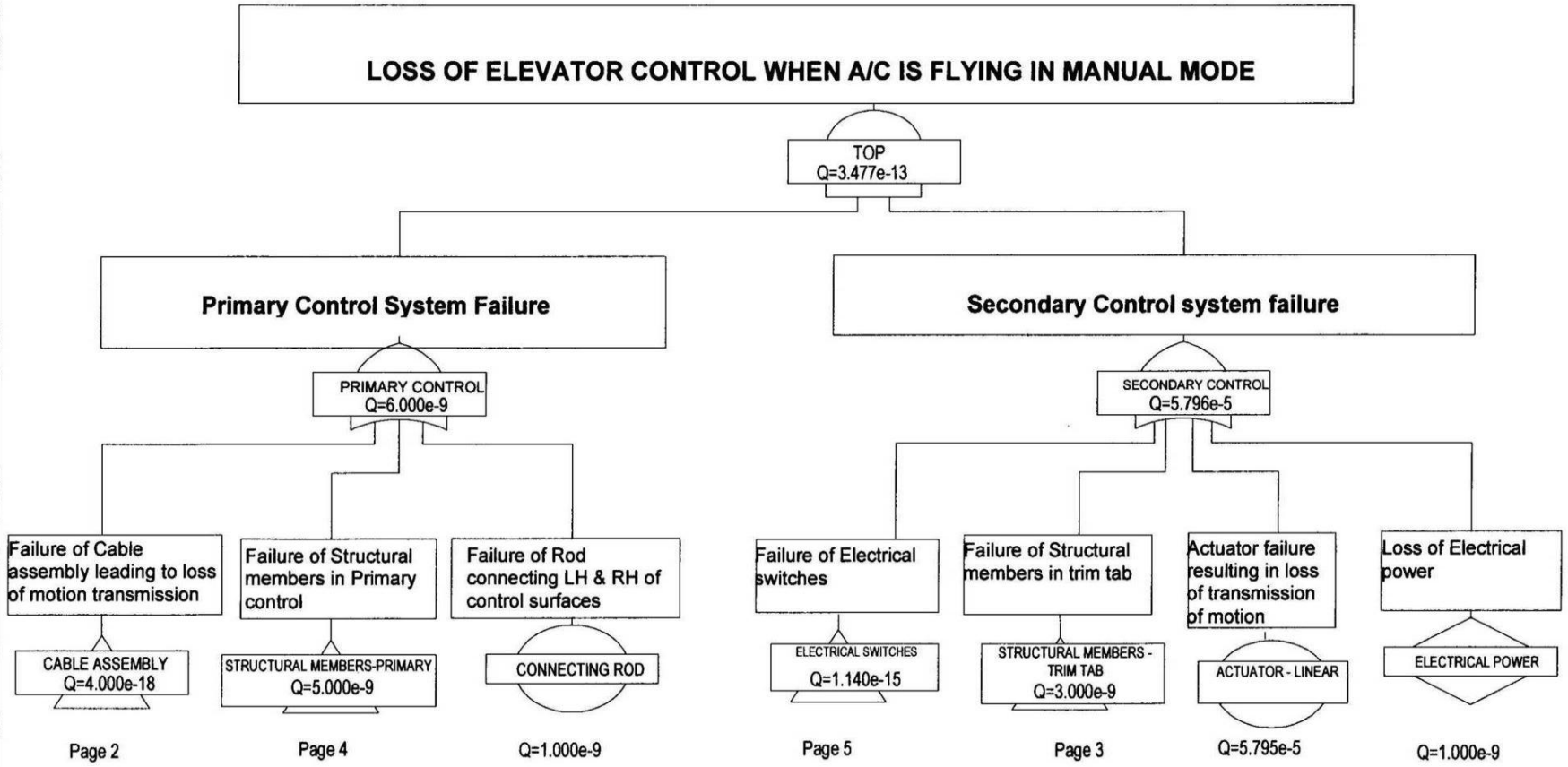
1. DEV G RAHEJA, ASSURANCE TECHNOLOGIES
   Mc GRAW-HILL INC, 1990
2. RELIABILITY REPORTS OF JAGUAR, TORNADO, LCA
3. SYSTEM SAFETY PROGRAMME, MIL-STD-882
4. MAINTAINABILITY PROGRAMME REQUIREMENTS , MIL-STD-470A
5. MAINTAINABILITY PREDICTION, MIL-HDBK-4T2
6. MAINTAINABILITY REQUIREMENTS FOR AVIONICS, ELECTRONIC
   SYSTEMS AND EQUIPMENT, MIL-STD-2084
7. MAINTAINABILITY VERIFICATION, MIL-STD-471
8. INTERCHANGEABILITY AND REPLACEMENT , MIL-I-8500
9. INTEGRATED AIRFRAME DESIGN TECHNOLOGY, AGARD-R-814

FAILURE MODE EFFECT ANALYSIS

Aircraft : [redacted] Item Ident. and Part No. : Item No. 01 in Fig. 1 Study Sheet No. : 1
System : FUEL Location on Aircraft : Collector tank
Sub-system :
Equipment : Booster Pump (01) RH/LH tank

Case	Type of Failure	Condition which modify effects of failure	Failure effect under conditions of column 3 a) on equipment b) on system c) on aircraft	Grade	Detection or warning for failure	Action to be taken		Failure rate (No. of failure per hour)	Remarks
						Air crew	Ground crew		
1.1	Fails to supply fuel to the engine (RH)	During DI/ starting phase	a) Booster pump u/s b) Fuel cannot be supplied to the RH side engine c) A/C cannot be cleared for flight	E	Amber warning in the cockpit about the failure of Booster pump	Abort engine starting	M1	6.7×10^{-7}	
1.2	Fails to supply fuel to the engine (LH)	During DI/ starting phase	a) Booster pump u/s b) Fuel cannot be supplied to the LH side engine c) A/C cannot be cleared for flight	E	Amber warning in the cockpit about the failure of Booster pump	Abort engine starting	M1	6.7×10^{-7}	
1.3	Booster pump failed to supply fuel to the engine and emergency pump is u/s (double failure)	Flight	a) Both booster and emergency pumps are u/s on the affected side b) Fuel cannot be supplied to engine from affected tank c) Flame out of the affected engine	E	Amber warning in the cockpit about the failure of both the pumps in one wing	Select booster pump of the other side tank to meet the fuel require-ment of both the engines		6.7×10^{-7}	Since both booster and emergency pumps of the other tank are capable of supplying fuel to both the engines through manual selection of cross feed valve (18) engine flame out will not happen

FTA No. 2 : LOSS OF ELEVATOR CONTROL WHEN A/C IS FLYING IN MANUAL MODE



- Uninterrupted fuel flow to engine
- Unimpaired by maneuver temperature and altitude effects
- Fuel pressurization and venting to ensure transfer, defuel and refueling operations
- Accurate gauging of fuel quantity
- Absence of common cause failures and single point failures

FUEL SYSTEM, RELIABILITY DESIGN DRIVERS

FUNCTIONAL HAZARD ANALYSIS

System : Environmental Control System
Sub-system : Air Conditioning System

Item No.	Functional Failure	Flight Phase	Effect on Aircraft	a. Crew Recognition b. Crew Action c. Workload on Crew	Criticality	Requirement	Required Probability	Remarks
1.	Loss of ECS pack, emergency air supply & ram air supply (Triple failure)	Flight (over mountain worst case)	Loss of all airflow into cabin	a) Cabin altitude increases b) Decend to an unpressurized level. Deploy oxygen masks and land as early as possible	Major	FAR 25.1309 FAR 25.831 FAR 25.1441 FAR 25.1443 FAR 25.1445 FAR 25.1449 FAR 25.1453	IE-05	Method of compliance: (i) Safety Assessment: FTA and system FMEA
2.	Complete loss of cabin temperature control	All	No aircraft effect, passenger discomfort will be there	a) Air temp. not normal even after operating temp. Control system manually b) If too cold, switch on the emergency air supply If too hot, decend to unpressurized altitude & use ram air supply c) Slight increase in work load	Minor	FAR 25.1309 FAR 25.831	IE-03	Method of compliance: (i) Safety assessment: FTA and system FMEA
3.	Smoke inside the cabin	All	Smoke in cabin, may result in passenger injury	a) Smoke in cabin b) Shut down ECS pack if smoke is coming from ECS system Decend below 15000 ft Rapidly depressurize A/C Open one emergency exit c) Significant increase in work load	Major	FAR 25.1309 FAR 25.831	IE-05	Method of compliance: (i) Safety assessment: FTA and system FMEA

FUNCTIONAL HAZARD ANALYSIS (a sample)

Haz. No.	Hazard Description	Flight Phase	Effect on Aircraft	Hazard Severity (A)	Probability Of Occur (B)	HRI (AxB)	Detection	Safety Provision	Revised HRI			Remarks
									Haz Severity (A)	Prob. Of Occur (B)	HRI (AxB)	
1	Loss of air data system	3,4,5	Flight control system cannot compute flight critical parameters. FCS in standby gain mode.	II Critical	D Remote	10	Warnings available	CLAW will revert to standby gain Standby instruments available for flight information	II	D	10	Acceptable with review (AWR). Method of compliance : FTA
2	Loss of flight control system	2,3,4,5	Actuators and other control system function not available	I Catastrophic	D (Remote)	8	Self evident	Fly into ejection envelope.	I	D	8	Undesirable (UD) Method of compliance : FTA
3	Loss of LES actuation in extended mode	2,3,4	Stability of the aircraft get affected.	II Critical	D (Remote)	10	Warning available	Nil	II	D	10	Acceptable with review (AWR). Method of compliance : FTA

Illustrative Examples for Various Elements of Product Assurance

1.	Installation Design	a. One hydraulic system breakage leading to failure of second hydraulic system b. Inconsistent behavior of brake parachute under cross wind conditions
2.	Threshold in respect of BIT	Frequent PBIT failure leads to abort take off
3.	Absence of segregation of signal and power cables	Multiple failure of FCS
4.	False alarm	Multiple path for undercarriage status indication leads to high rate of false alarm
5.	Zonal design	Water particles dripping over battery from ECS water extractor
6.	Single point failure	A crack in PTU leading to failure of redundant hydraulic system
7.	Incorrect adjustment procedure in safety system	Inadvertent jettison of ejection seat
8.	Incorrect estimation of fatigue strength	Dis-integration of Radome
9.	In correct test procedure on engine flame out	Unintended stalling in flight
10.	Inadequate structural strength	Panels flew in air