



GEA Tianjin / 中国民航大学中欧航空工程师学院

SB 503 - Avionics Technologies

1- introduction to Avionics Technologies

1-1 Introduction to Safety & Systems

1-2 Avionics Certification Process including applicable Standards

1-3 Human Factors Prospectives

1-4 Avionics System Architectures (Logical- Functional)

1-5 Avionics Systems & [Missions- Functions - Resources]

Professor: Hervé GOUTELARD (Contractor ENAC/Sup'Aéro)

Thales Avionics

GEA Tianjin / 中国民航大学中欧航空工程师学院

Objectives : To provide the engineers with basic safety notions
and to anticipate System Architecture presentations

- Part 1 - Introduction to Safety concepts
 - Generalities
 - Aircraft airworthiness
- Part 2 – Avionics systems : design for safety
 - Safe architectures
 - Candidate architecture assessment
- Part 3 – Assessment of systems safety
 - Process guidelines
 - Dysfunctional analyses, Reliability, DAL
- Conclusion



GEA Tianjin / 中国民航大学中欧航空工程师学院

Part 1 – Introduction to « Safety » concepts

- Contents :
 - Generalities
 - Historic of safety
 - Risk theory and Management
 - Aviation accidents statistics
 - Aircraft airworthiness
 - Aviation safety regulation
 - Aviation Risk
 - Safety requirements for large commercial aircrafts
 - A/C airworthiness in the future



GEA Tianjin / 中国民航大学中欧航空工程师学院

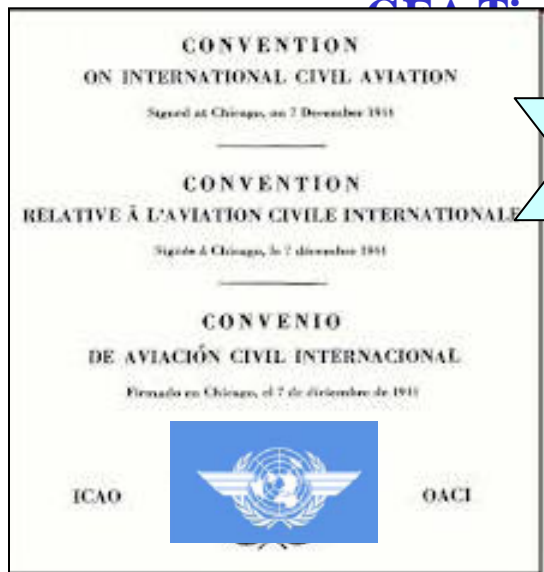
Generalities : Safety historical background

Late development of reliability / safety techniques in Engineering

- 1900-1930 : Approach linked to material resistance & life-time limit
- 1930s : First statistical studies in Aviation
- 1940s : Introduction of prediction reliability models
 - 1944 : *Convention of Chicago on International Civil Aviation*
- 1950-60s : Boom of the discipline with the arrival of electronics
- 1960-70s : Introduction of norms & regulations for safety analyses
- 1970-80s : Multi-domain diffusion, Human Factors

CEAT Tianjin / 中国民航大学中欧航空工程师学院

International Civil Aviation Organisation (ICAO) :



**Chicago
1944**

**191
States**

- A safe and orderly development of international civil aviation
- International Air transport services established on the basis of equality of opportunity and operated soundly and economically
- Specify minimum requirements to ensure safety
- Member states :
 - Rules and Implementations
 - Technical Requirements
 - National Authorities / Administration / Agency

Articles 29, 31 & 33

**1 / Must have a Certificate of
Airworthiness (C of A)**

**2 / C of A delivered by the
State of Registry**

N-603JB

**3/ Requirements
= or > ICAO**

FAR, CS

ICAO

**Safety is a public right
Aviation is global**

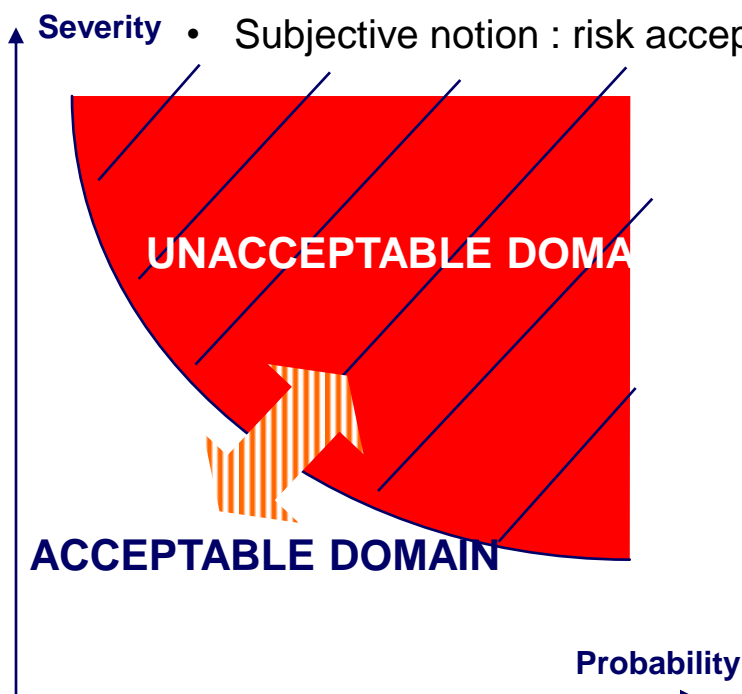
**C of A Recognised
> Flight-Over authorised**

GEA Tianjin / 中国民航大学中欧航空工程师学院



Generalities : Risk theory

- Risk theory :
 - Hazard => Risk => Event (Accident/Incident : occurrence of the risk)
 - Risk criticality = risk probability x event severity
 - Notion of individual risk acceptability
 - basic rules = more it is serious, less it should occur
 - Subjective notion : risk acceptance vs. potential benefits



*Common risk acceptance level :
fatal accident = 1 / 1 million hours*

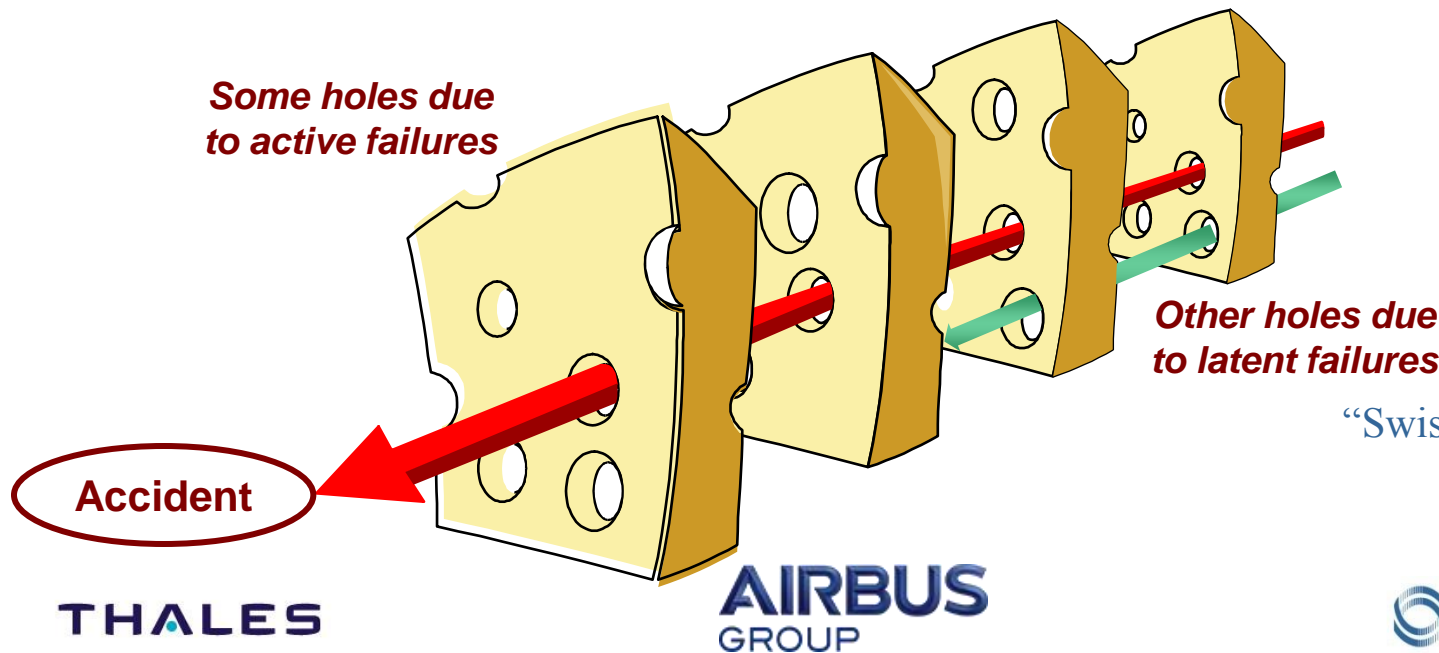
Chances of death per Leisure Activities	per million hrs
Skydiving	128,71
Flying (General Aviation)	15,58
On-road Motor Cycling	8,8
Scuba Diving	1,98
Living (all causes of death)	1,53
Passenger cars	0,47
Water skiing	0,28
Bicycling	0,26
Flying (scheduled domestic airlines)	0,15
Traveling in a School Bus	0,022

GEA Tianjin / 中国民航大学中欧航空工程师学院



Generalities : What is an accident ?

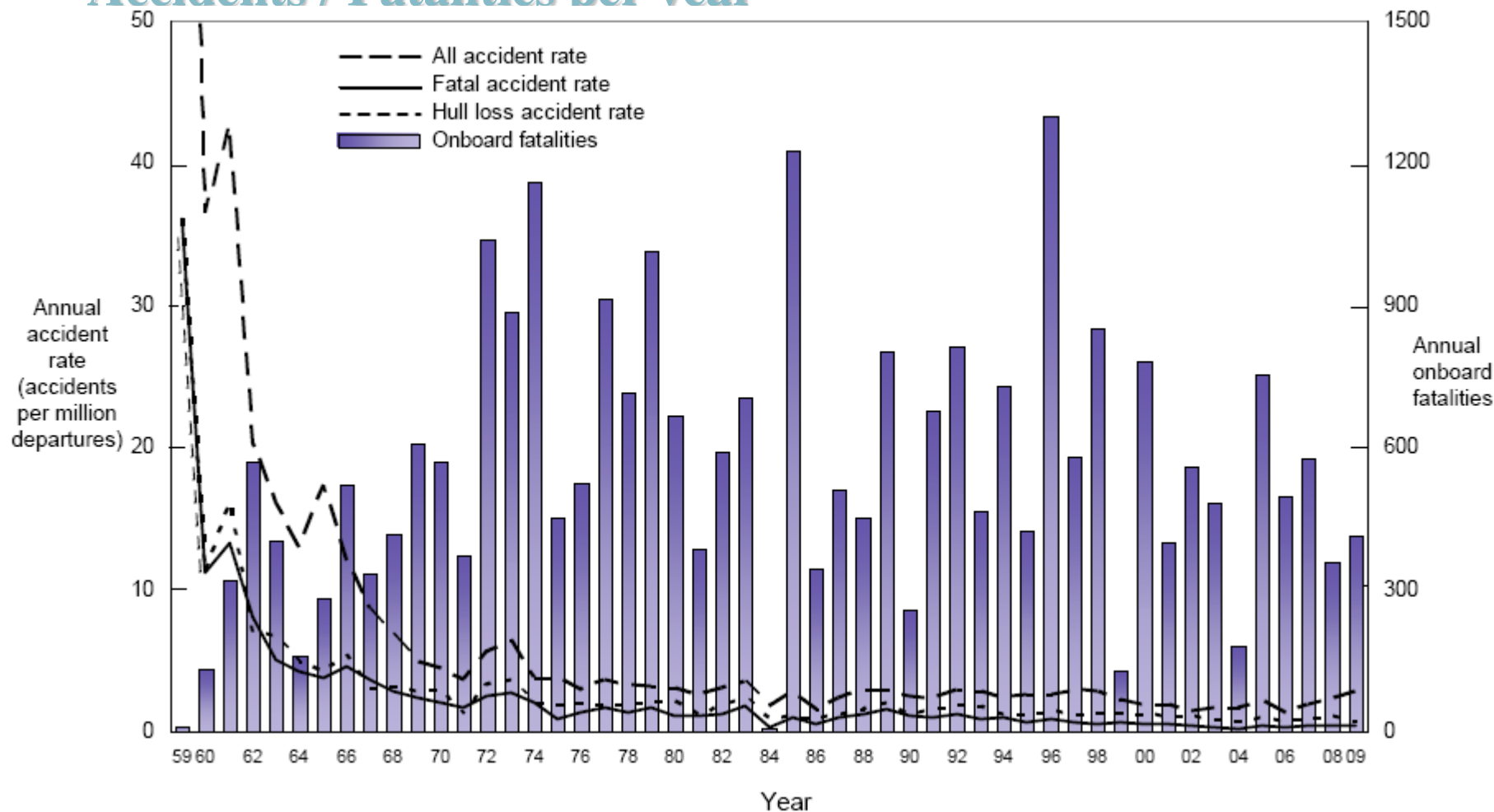
- An airplane accident (ICAO definition) is :
 - The occurrence of an event which effects are :
 - **Hull loss** (airplane substantial damage, missing or inaccessible),
 - **Fatal accident** (onboard fatalities : death of passengers or crew),
 - Serious injury to one or more person.
 - During operation of an A/C (from boarding to disembarkation),
 - Often a scenario resulting from several causes combination :
 - Successive holes into layers of defenses



“Swiss Cheese” model
(J.T Reason)

GEA Tianjin / 中国民航大学中欧航空工程师学院

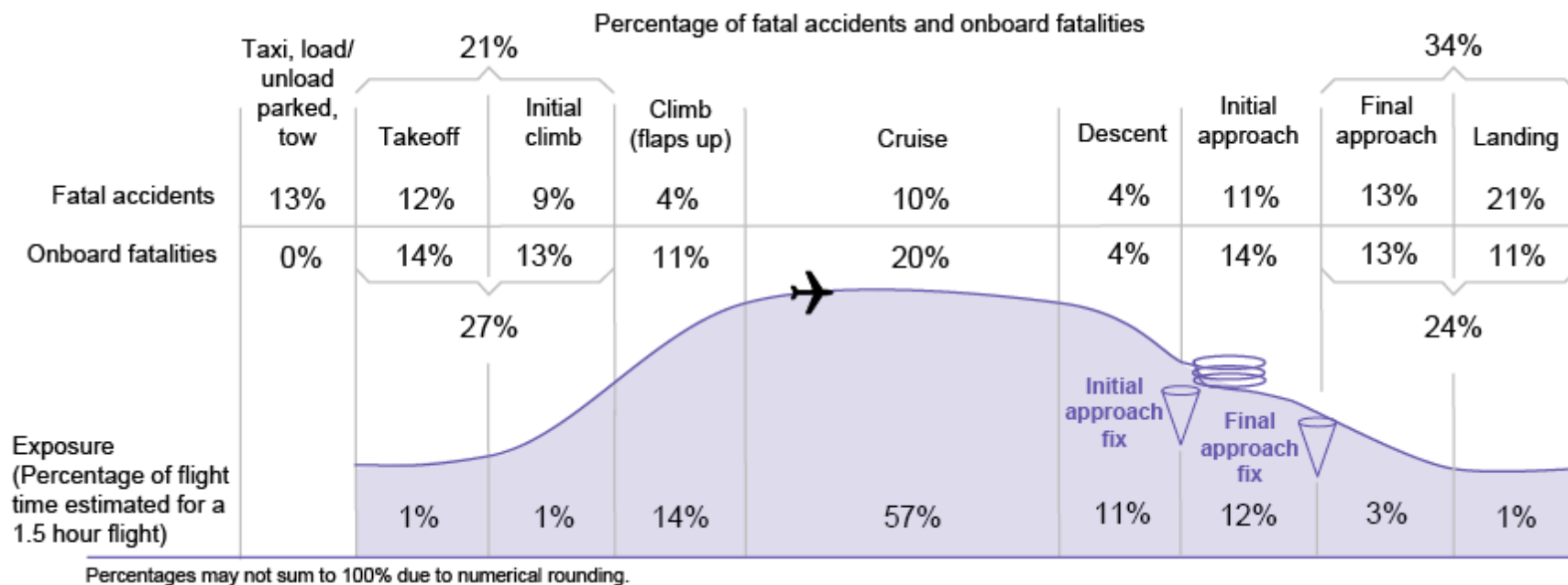
• Accidents / Fatalities per year



Source : Boeing – Statistical Summary of Commercial Jet Airplane
Accidents – Worldwide Operations – 1959 -2009

GEA Tianjin / 中国民航大学中欧航空工程师学院

Accidents / Fatalities per Flight Phase



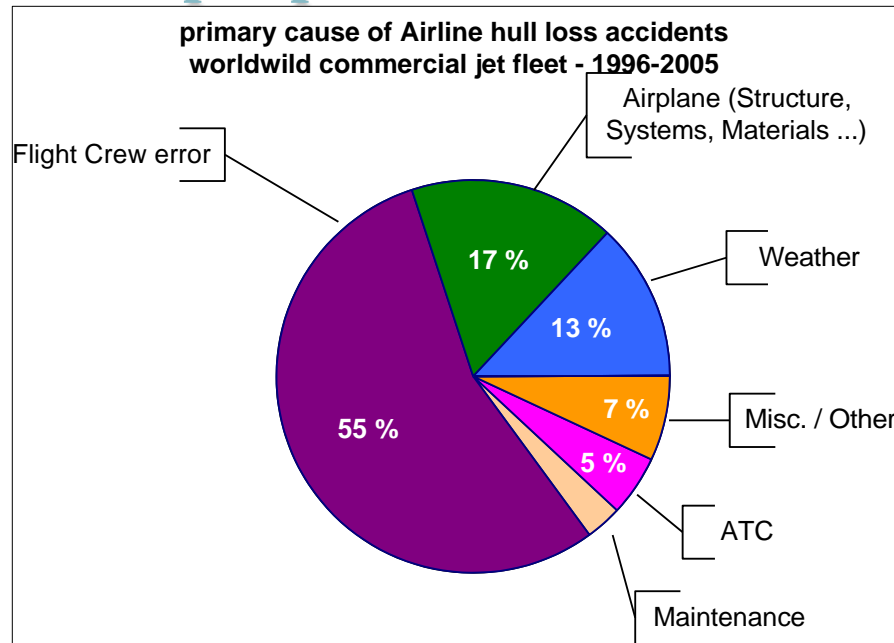
Source : Boeing – Statistical Summary of Commercial Jet Airplane Accidents – Worldwide Operations – 1959 -2009

GEA Tianjin / 中国民航大学中欧航空工程师学院

Generalities : Aviation accidents statistics



• Accident per prominent causes



- Source : Boeing – Statistical Summary of Commercial Jet Airplane Accidents – Worldwide Operations – 1959 - 2005

- Most important = Human Errors ($\approx 65\%$)
 - Flight Crew + Maintenance Crew + Air Traffic Control
- Airplane = 17 % :
 - Structure
 - Systems
 - Hazardous Materials (Fuel ...) & Particular Risks (Fire, ...)

Systems contribution $\approx 10\%$



GEA Tianjin / 中国民航大学中欧航空工程师学院

Part 1 – Aircraft airworthiness

- Part 1 – Introduction to Safety concepts
 - Generalities
 - Aircraft airworthiness
 - Aviation safety regulation
 - Aviation Risk
 - Safety requirements for large commercial aircrafts
 - A/C airworthiness in the future



Main civil air transportation Authorities



GEA Tianjin / 中国民航大学中欧航空工程师学院

– EUROPE **EASA** European Aviation Safety Agency (2002)

- FR DGAC
- UK CAA
- DE LBA
- NL RLD
- ES DGAC-S
- IT ENAC



– US **FAA** Federal Aviation Administration



– CANADA **TCCA** Transport Canada Civil Aviation



Transport
Canada

Transports
Canada

– BRESIL **ANAC**



– RUSSIE **IAC-AR** Interstate Aviation Committee–Aircraft Register



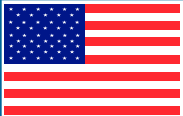

– CHINE **CAAC**



GEA Tianjin / 中国民航大学中欧航空工程师学院

A/C airworthiness : Aviation safety regulations

- International aeronautical regulation

2 great families	 Federal Aviation Administration (FAA)	 European Aviation Safety Agency (EASA)
SAFETY regulations	Federal Aviation Regulations (FAR) 23-25-27-29 § 1309	Certification Specifications (CS) CS 23-25-27-29 § 1309
Means of Compliance	Advisory Circulars (AC) AC 25.1309	Acceptable Means of Compliance (AMC) AMC25.1309
Specific to systems	AC25-11 ...	AMC25.11 (Displays) CS-AWO 268 (RA)

GEA Tianjin / 中国民航大学中欧航空工程师学院

EASA CS 25.1309 Equipment, Systems and Installations

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that (see AMC 25.1309(b))

- (1) Any catastrophic failure condition is extremely improbable; and
- does not result from a single failure; and
- (2) Any hazardous failure condition is extremely remote; and
- (3) Any major failure condition is remote.

Occurrence				
	$10^{-5}/\text{hour}$	$10^{-7}/\text{hour}$	$10^{-9}/\text{hour}$	
Consequences	Probable	Remote	Extremely remote	Extremely improbable
Minor	ACCEPTABLE			
Major				
Critical	UNACCEPTABLE		ACCEPTABLE	
Catastrophic				

Severity Classification	FAA	Minor	Major	Severe Major	Catastrophic
	EASA			Hazardous	
Potential Accident Effects	Aircraft	Slight reduction in safety margins or functional capabilities	Significant reduction in safety margins or functional capabilities	Large reduction in safety margins or functional capabilities	hull loss
	Flight Crew	Slight increase in crew workload, such as routine flight plan changes	Significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew	Physical distress or excessive workload such that the flight crew cannot perform their tasks	Fatalities or incapacitation
	Occupants	Some physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a relatively small number	Multiple fatalities
Probability requirement	FAA	Probable	Improbable		Extremely improbable & no single failure
	EASA		Remote	Extremely remote	
Qualitative probability terms		one or more times during the entire operational life of each aeroplane	several times during the total operational life of a number of aeroplanes	- not anticipated to occur to each aeroplane during its total life - a few times during the total operational life of all aeroplanes	not anticipated to occur during the entire operational life of all aeroplanes

GEA Tianjin / 中国民航大学中欧航空工程师学院

Severity classification : Example

- Which severity for risks linked to Landing Gear ?
 - Annunciated inability to retract any Landing Gear ?
 - Annunciated loss of extension of any Landing Gear ?
 - Collapse of any Landing Gear :



• Nose L/G collapse ?

• Main L/G collapse ?

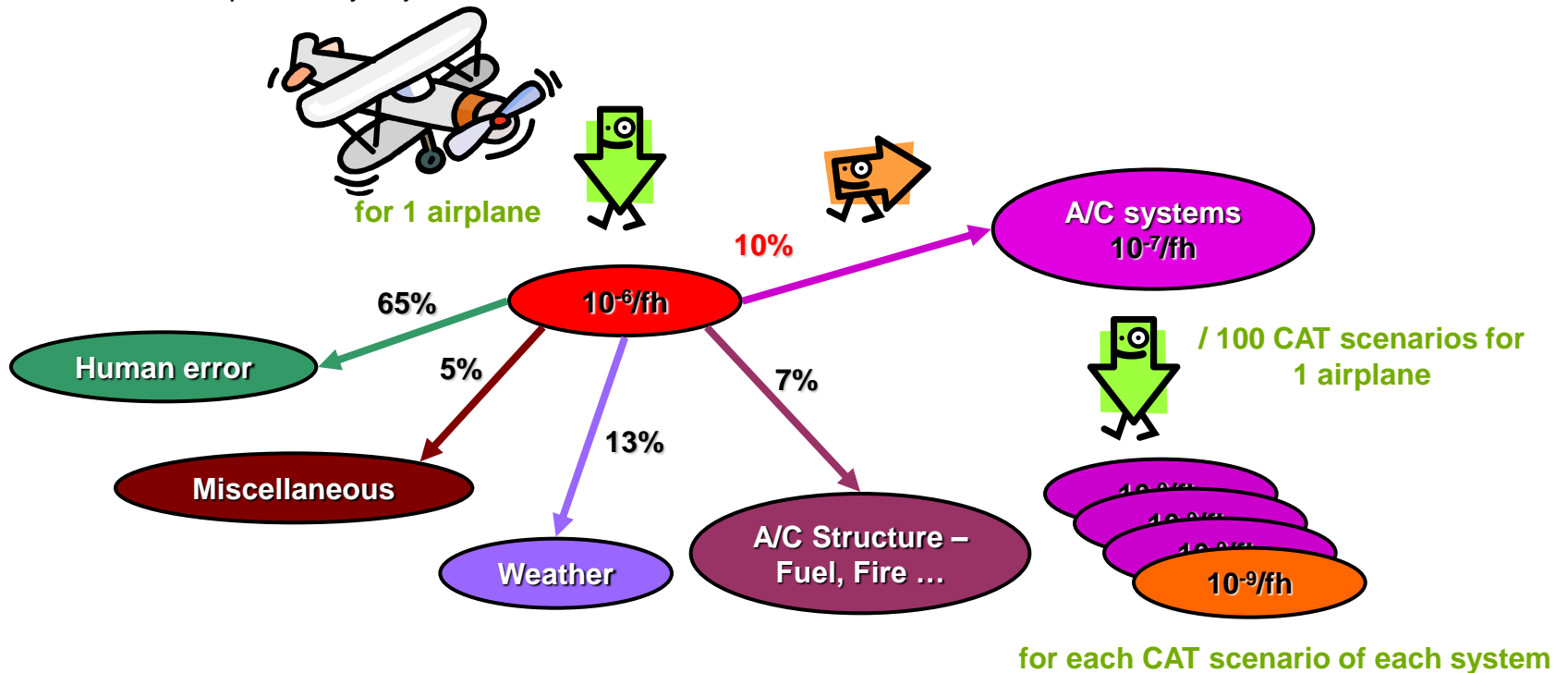


GEA Tianjin / 中国民航大学中欧航空工程师学院

Acceptability of Aviation risk

A/C historical statistics =>
Fatal accident occurrence rate < $1/10^6$ flight hours

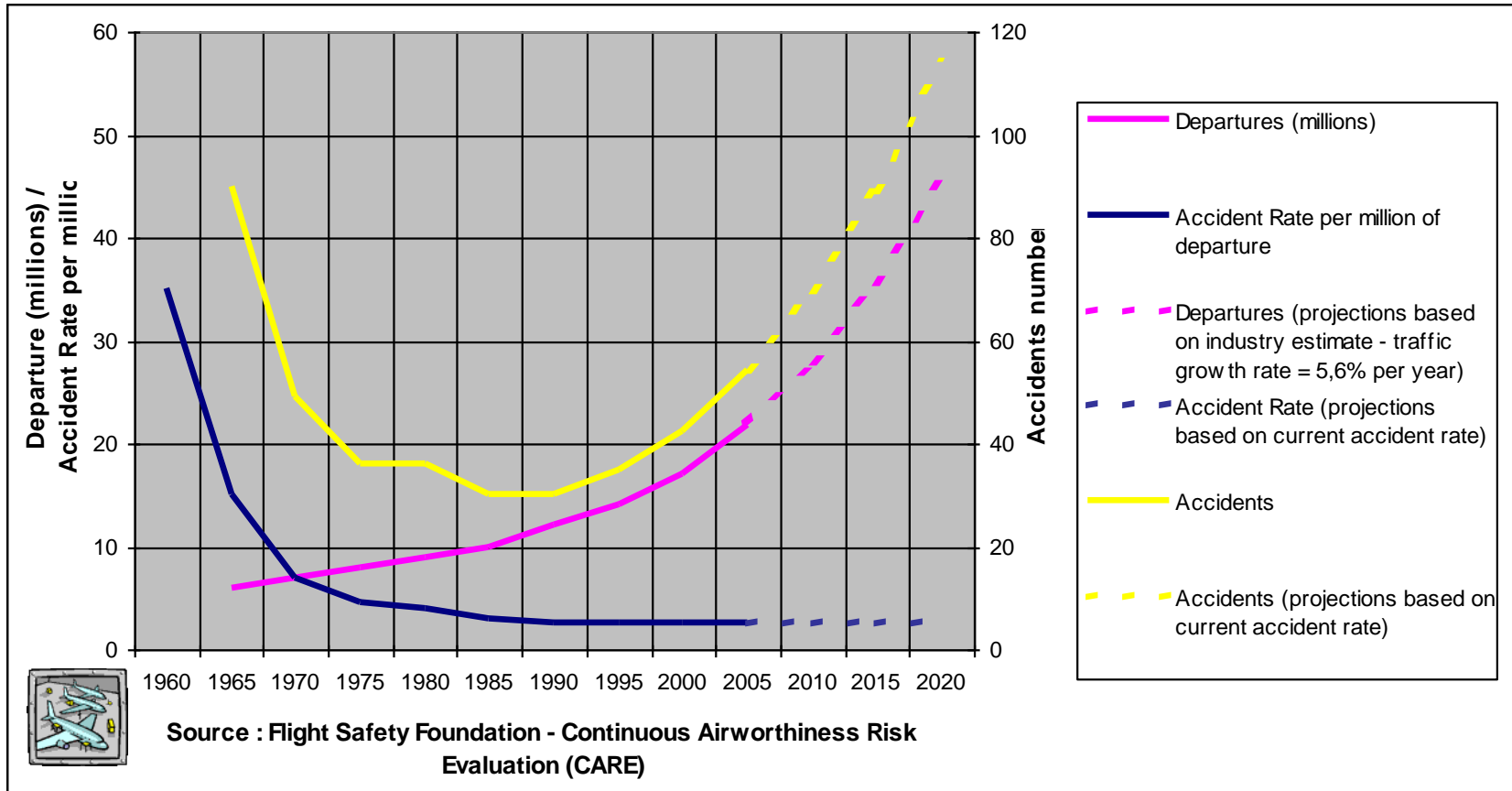
- Allocation of a probability objective for fatal accidents



Catastrophic risk = 10^{-9} / FH (AMC 25.1309)

GEA Tianjin / 中国民航大学中欧航空工程师学院

- The trend of commercial aviation



Challenges : Traffic growth & perception of risk => evolution of objectives ?



GEA Tianjin / 中国民航大学中欧航空工程师学院

Part 2 – Avionics systems : Design for safety

- Part 1 – Introduction to Safety concepts
- Part 2 – Avionics systems : Design for safety
 - Basement of safe architectures
 - Candidate architecture assessment
- Part 3 – Assessment of systems safety
- Conclusion

GEA Tianjin / 中国民航大学中欧航空工程师学院

Terminology – Safety performances



- Failure effect types

Failure effect type	Integrity loss	Availability loss
Effect on system	System malfunction	Loss of system function
Potential Causes	<ul style="list-style-type: none"> - Erroneous inputs acquisition, - Erroneous computation, - Erroneous outputs transmission ... 	<ul style="list-style-type: none"> - Loss of inputs / outputs, - Loss of core processing, power supply ...
Example of consequences	<ul style="list-style-type: none"> - Erroneous display - Erroneous not expected behavior - False or loss of alerts - Surface hardover 	<ul style="list-style-type: none"> - Power loss - Loss of display - Loss of alerts - Surface jamming
Compensation means	Voting, Comparison, Continuous monitoring (watchdog, EDC, ...)	Redundancy, Reconfiguration, Continuous monitoring (refresh, validity check, ...)

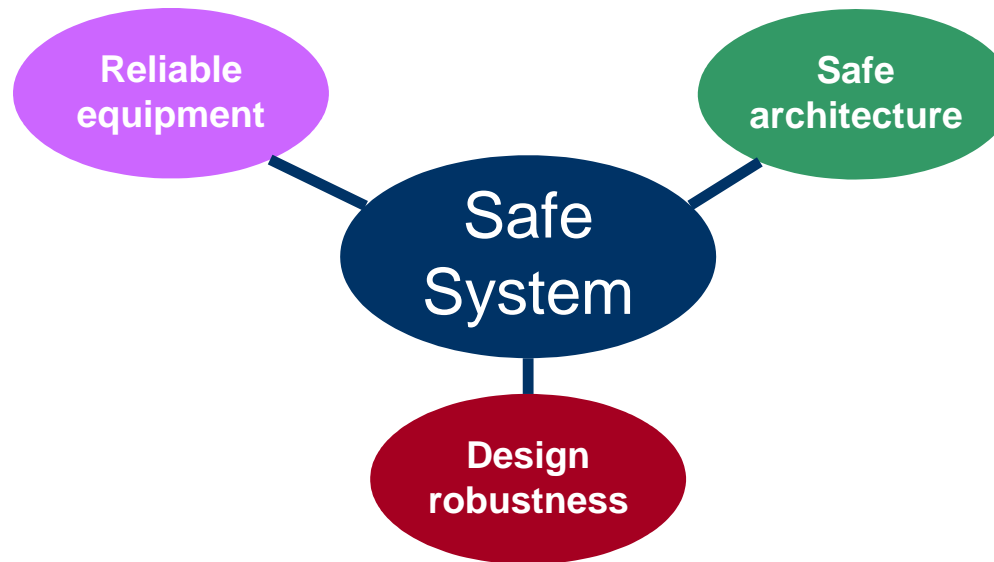
GEA Tianjin / 中国民航大学中欧航空工程师学院

Design for safety

- What is a Fail Safe system ?
- Upon failure occurrence, the system shall fail in a predictive SAFE state

2 main families :

- **“Fail-Passive”** : system is disabled upon failure occurrence
- **“Fail-Operational”** : system remains operational upon failure occurrence



GEA Tianjin / 中国民航大学中欧航空工程师学院

■ Basic definitions:

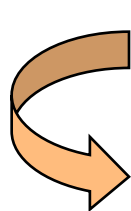
Reliability / Failure Rate (model)



● Reliability:

$R(t)$ = Reliability associated to a duration $(0, t)$ = Probability to survive at « t » (no unit)

● Failure rate: Expressed in « hours »



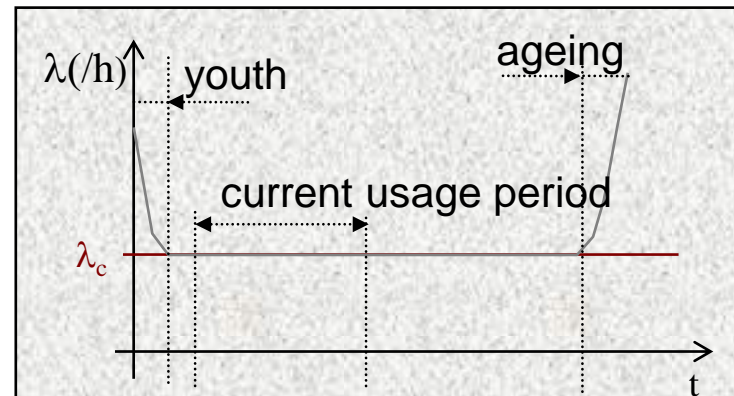
$$\lambda(t) = -\frac{1}{R(t)} \times \frac{dR(t)}{dt}$$

therefore :

$$R(t) = e^{-\int_0^t \lambda(\tau) d\tau}$$

Probability that a « working unit » at « t instant » encounters a failure between $[t, t+dt]$: $P(t) = \lambda(t) dt$

■ Density of probability for an electronics component to fail (see figure below)



GEA Tianjin / 中国民航大学中欧航空工程师学院

Reliability (model)



- For Electronics components, failure rate is a constant value
- In major study cases $\lambda(t) \ll 1$, by approximation, one can state:

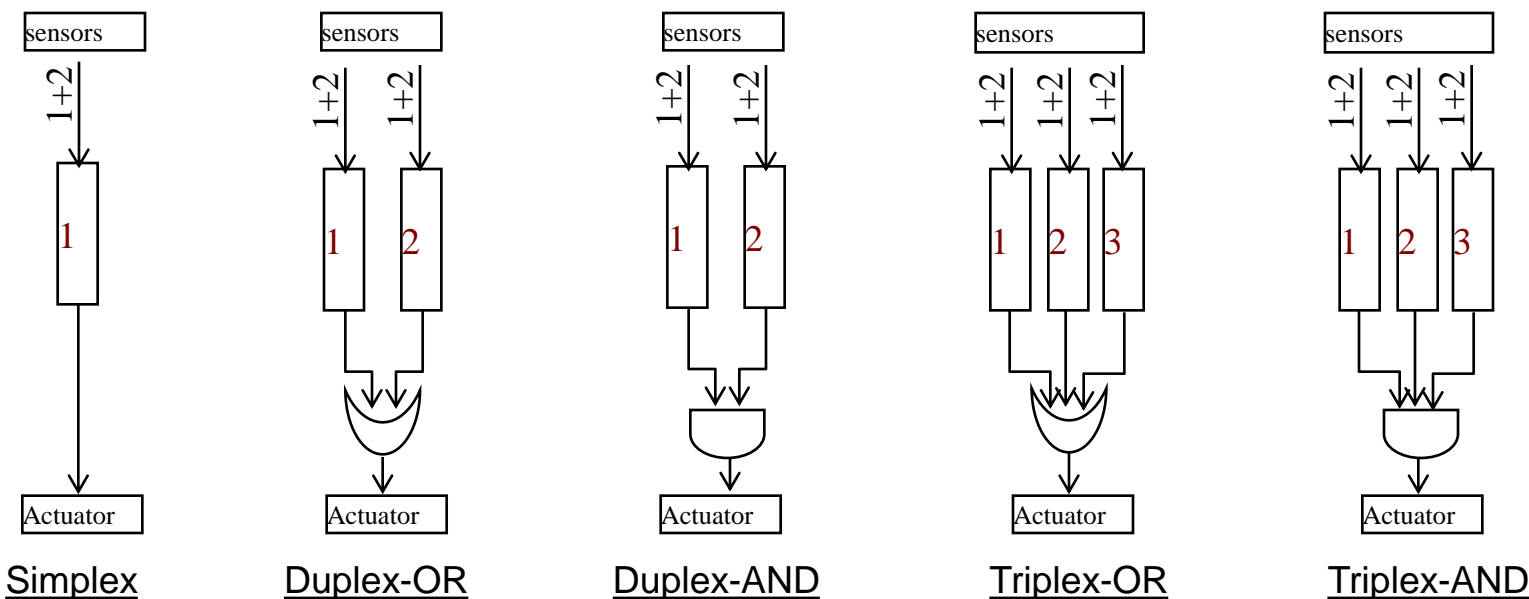
$$R(t) = e^{-\int_0^t \lambda(\tau) d\tau} = e^{-\lambda t} \approx 1 - \lambda t$$

$$P(t) = 1 - R(t) \approx \lambda t$$

- $t = T_0$ = Mission duration (1 to 10 h) $\lambda(t) \ll 1$
- $t = T_{\text{post}}$ = Elapse time between two POSTs (say ~ 10 to 100h) $\lambda(t) \ll 1$
- $t = T_M$ = Max. duration between two maintenance party (10 to 500h)
 $\Rightarrow \lambda(t) \ll 1$
- Sleeping failure:
 $\lambda(t) \sim 1 \Rightarrow$ Need to keep the exponential term through the probability computation

GEA Tianjin / 中国民航大学中欧航空工程师学院

Examples: Simple / double / triple Chains



architecture type	Without prior failure				After one single failure				Comment
	Loss		Integrity		Loss		Integrity		
Simplex	λ	4,07E-05	λ_{nd}	2,00E-06	-	-	-	-	
Duplex-OR	$\lambda^{2 \cdot T_0}$	1,66E-08	$2\lambda_{nd}$	4,00E-06	λ	4,07E-05	λ_{nd}	2,00E-06	after one channel failed = simplex
Duplex-AND	2λ	8,14E-05	$\lambda_{nd}^{2 \cdot T_{exp}}$	4,00E-10	-	-	-	-	
Triplex-OR	$\lambda^{3 \cdot T_0^2}$	6,74E-12	$3\lambda_{nd}$	6,00E-06	$\lambda^{2 \cdot T_0}$	1,66E-08	$2\lambda_{nd}$	4,00E-06	after one channel failed = duplex-OR
Triplex-AND	3λ	1,22E-04	$\lambda_{nd3} \cdot T_{exp}^2$	8,00E-14	-	-	-	-	

GEA Tianjin / 中国民航大学中欧航空工程师学院



Architectures designation
not normalized

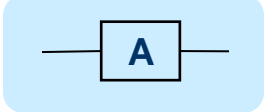
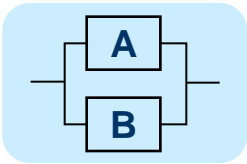
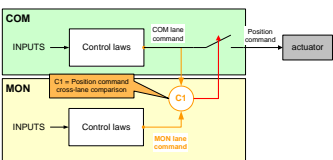
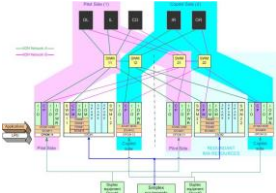
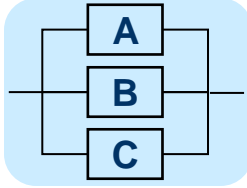
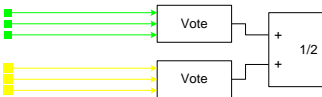
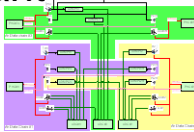
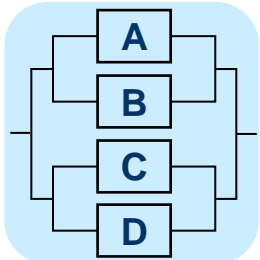
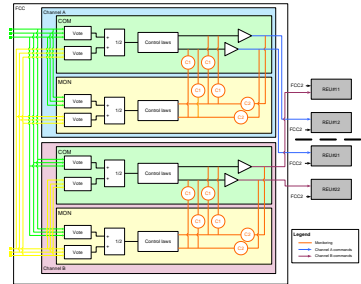
		Integrity requirement MAJOR	Integrity requirement HAZARDOUS - CATASTROPHIC
Availability requirement	MIN < $10^{-3}/h$	Simplex $loss = \lambda / integ. = \lambda i$	COM/MON $loss = 2. \lambda / integ. = \lambda i^2$
	MAJ < $10^{-5}/h$ HAZ < $10^{-7}/h$	Dual / Duplex-OR $loss = \lambda^2 / integ. = 2. \lambda i$	Dual COM/MON $loss = 4. \lambda^2 / integ. = 2 \lambda i^2$
	HAZ < $10^{-7}/h$ CAT < $10^{-9}/h$	Triplex-OR (3) $loss = \lambda^3 / integ. = 3. \lambda i$	Triple COM/MON $loss = 8. \lambda^3 / integ. = 3 \lambda i^2$
	CAT < $10^{-9}/h$	Quadruplex-OR (4) $loss = \lambda^4 / integ. = 4. \lambda i$	Quad COM/MON $loss = 16. \lambda^4 / integ. = 4 \lambda i^2$
			Triplex-AND $loss = 3. \lambda^2 / integ. = 3 \lambda i^2$
			Double Triplex $loss = 9. \lambda^4 / integ. = 6 \lambda i^2$

COM / MON based

Voter based

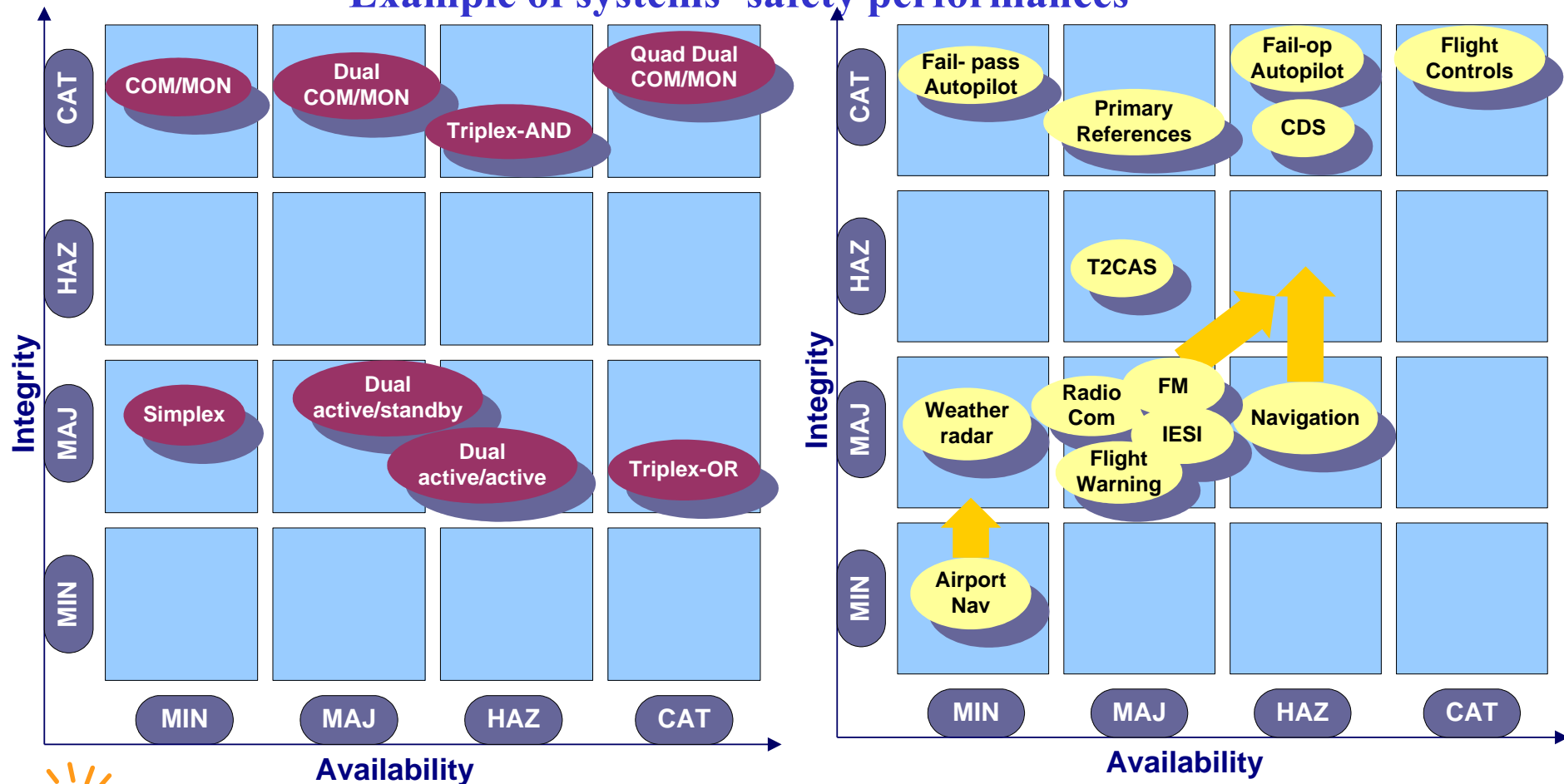
- Assumption on computing h/w platform : $10\ 000\ FH < MTBF < 100\ 000\ FH \sim 10^5$
 - Integrity: $10^{-7}/h < \lambda$ Integrity (Undetected erroneous computation) < $10^{-5}/h$
 - Availability: $10^{-5}/h < \lambda$ Loss (loss) < $10^{-3}/h$
- For illustration purpose only: Not meant to be exhaustive, neither valid in all cases
 - Dissimilarity aspects / Hidden failures issues not addressed

GEA Tianjin / 中国民航大学中欧航空工程师学院

<u>Architectures</u>	Integrity criteria : Comparison, voters	Availability criteria : Redundancy or backup
Simplex 		
Duplex 	COM/MON 	Dual active-active active-standby 
Triplex 	Triplex-AND 	Triplex-OR redundant 3 active 2 active-standby 1 active – 2 standby 
Quadruplex 	<ul style="list-style-type: none"> - Dual COM/MON (4 channels) - Quad COM/MON (8 channels) 	

GEA Tianjin / 中国民航大学中欧航空工程师学院

Example of systems' safety performances



A “safe architecture” design depends on objectives

GEA Tianjin / 中国民航大学中欧航空工程师学院

Safety Requirements ↔ Candidate SW architectures

- Strategy against systematic errors (includes S/W ones)
 - No possibility to quantify and apply reliability predictions
 - Effective defences are ensured by :
 - Safety architecture features
 - Redundancies (multiples versions of software)
 - Monitoring (COM/MON, voters)
 - Independence of critical from non-critical functions
 - » Physical segregation (through hardware) or
 - » Temporal / spatial partitioning
 - Implementation of quality in development process (DAL levels)
 - Dissimilarity :
 - Different specifications, coding team and languages,
 - Different compilers to generate executable code and asynchronous functioning.
 - Software robustness to environment best practices
 - Dysfunctional effects are taken into account through h/w FTA

GEA Tianjin / 中国民航大学中欧航空工程师学院

No single failure (1/2) ?



- Airworthiness = no single failure for CAT FC : **CS 25.1309** (b) (1) (ii)
- Notion of **Failure** versus **Error** :
 - **Error** are systematic faults introduced by human activity :
 - A mistake in specifications, design, manufacturing or installation leading to system faults,
 - A mistake in operating (flight crew) or during maintenance actions,
 - **Failure** are random hardware occurrences
 - which affect the operation of a component, part or element such that it can no longer function as intended (this includes both loss of function and malfunction).
- Best practices = reduction of “common modes” in an acceptable way
 - Shared components,
 - Common external sources, common aircraft services (e.g. power supply etc.)
 - **Error** affecting different similar S/W or complex H/W in the same way,
 - Environmental factors (temperature, vibration, lightning ...), physical installation in A/C face to intrinsic hazards (rotor burst, tyre burst, fire, electromagnetic impacts...)
 - Cascading / propagating failures.



GEA Tianjin / 中国民航大学中欧航空工程师学院

No single failure (2/2) ?

- Excluded failures (CS 25.1309) :
 - CS 25.671 Flight control system (c) (1), (c) (3)
 - CS 25.735 Brake system capability (b)
 - CS 25.810 Emergency egress assist means and escape routes (a)(1)v)
 - CS 25.812 Emergency lighting



GEA Tianjin / 中国民航大学中欧航空工程师学院

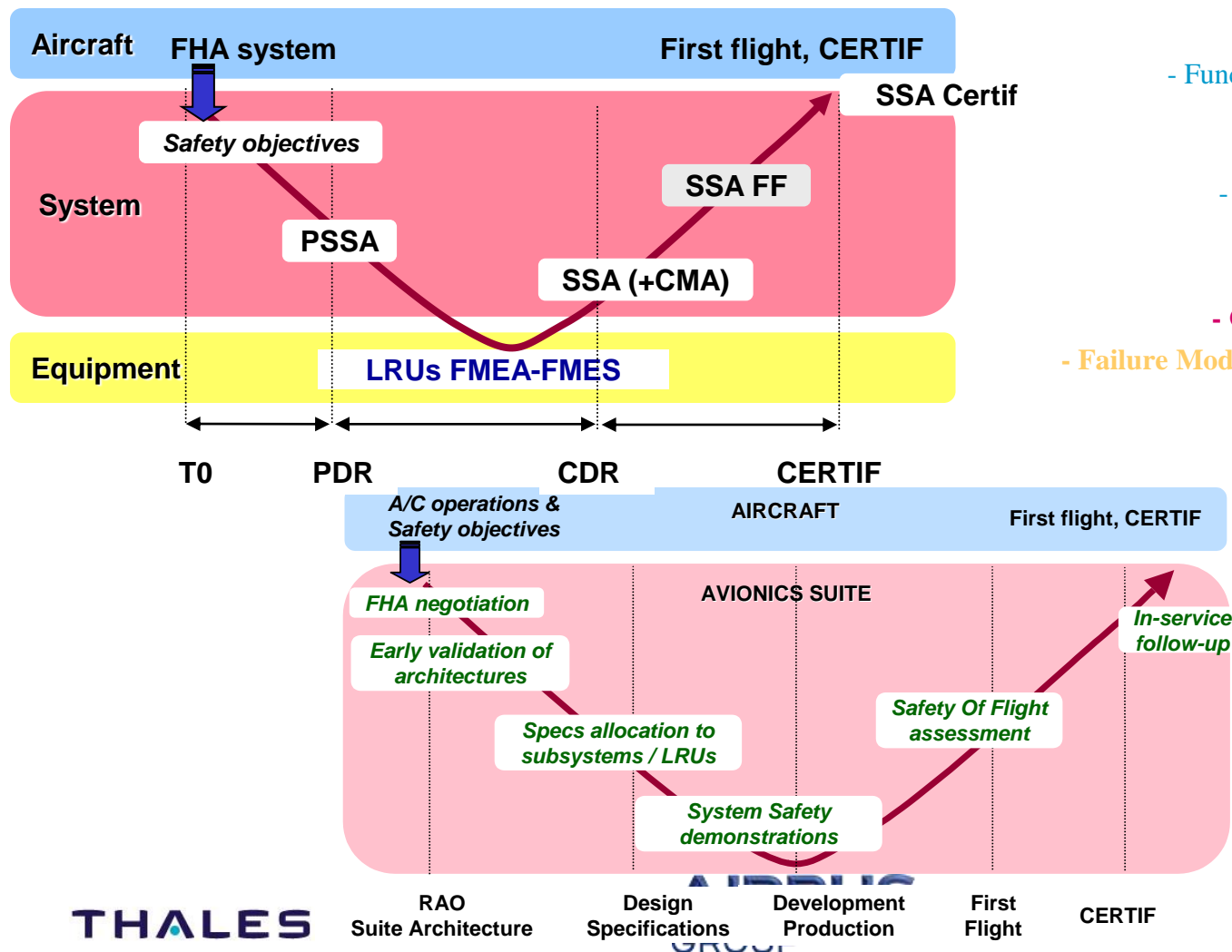
Part 3 – Systems safety Assessment

- Part 1 – Introduction to Safety concepts
- Part 2 – Avionics systems : design for safety
- Part 3 – Assessment of systems safety
 - Process guidelines
 - Dysfunctional analyses, Reliability
 - Development Assurance Level
- Conclusion

GEA Tianjin / 中国民航大学中欧航空工程师学院

Safety Assessment Process (ARP4761)

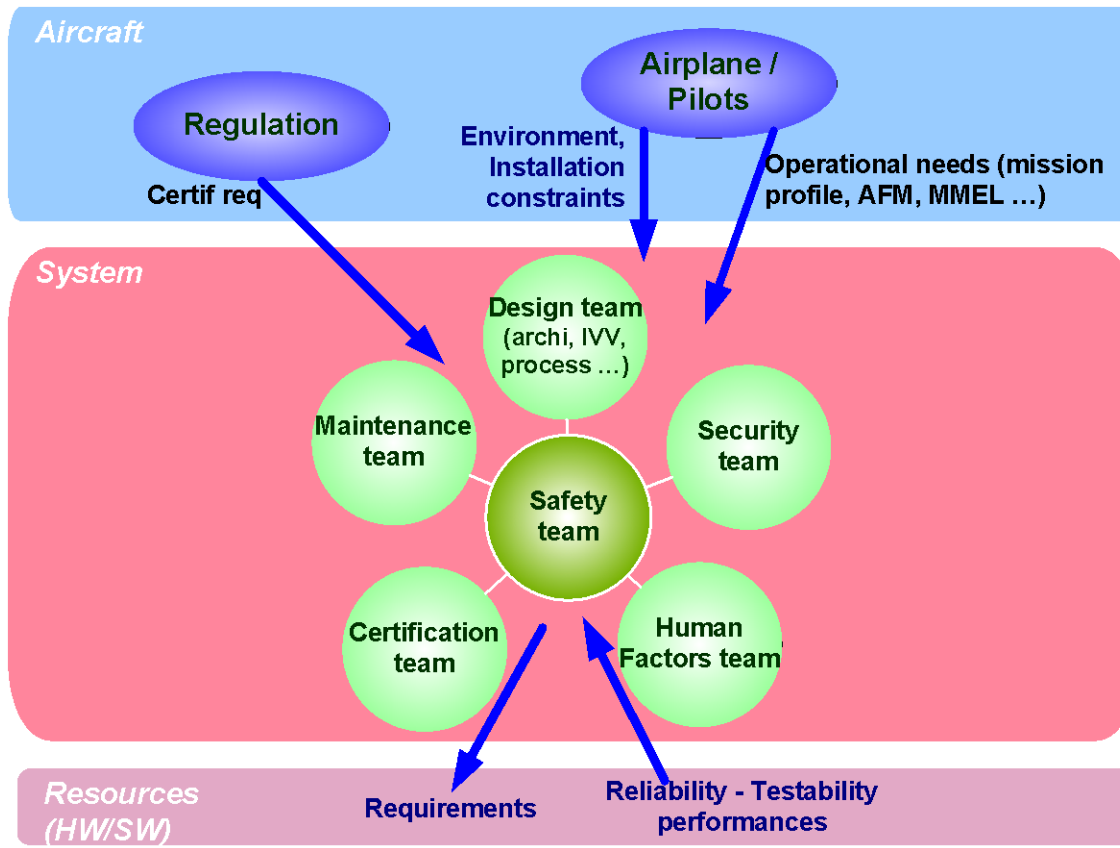
- Safety Analyses & Documentation



GEA Tianjin / 中国民航大学中欧航空工程师学院

Safety on-board

- System Engineering = Various & different skills in interaction





GEA Tianjin / 中国民航大学中欧航空工程师学院

Part 3 – Assessment of systems safety

- Part 1 – Introduction to Safety concepts
- Part 2 – Avionics systems : design for safety
- Part 3 – Assessment of systems safety
 - Process guidelines
 - Dysfunctional analyses, Reliability
 - Development Assurance Level
- Conclusion

GEA Tianjin / 中国民航大学中欧航空工程师学院

Dysfunctional analyses

- Fault-Tree analysis (FTA)
 - When this method is used ?
 - Top-down and deductive analysis
 - Mainly used for “complex” parts (system or sub-system analyses)
 - Qualitative analysis (scenarios, single failures, DAL allocation ...)
 - Justification of probability of occurrence of FHA feared events
 - Required inputs data ?
 - System architecture & intrinsic behavior
 - A/C environment conditions
 - Operational use of the system (cockpit + maintenance)
- Failure Modes & Effects analysis (FMEA)
 - Bottom-up and systematic analysis of single failures
 - Used at equipment level (FTA inputs)
 - Used at system level (demonstration of fail-safe criteria for CAT events)
- Common Modes Analysis (CMA) **(CAT and HAZ only)**
 - Verification of independence hypotheses made in FTA analysis
 - Assessment of single common ERRORS effects

GEA Tianjin Fault Trees Analysis 中国民航大学天津航空工程师学院

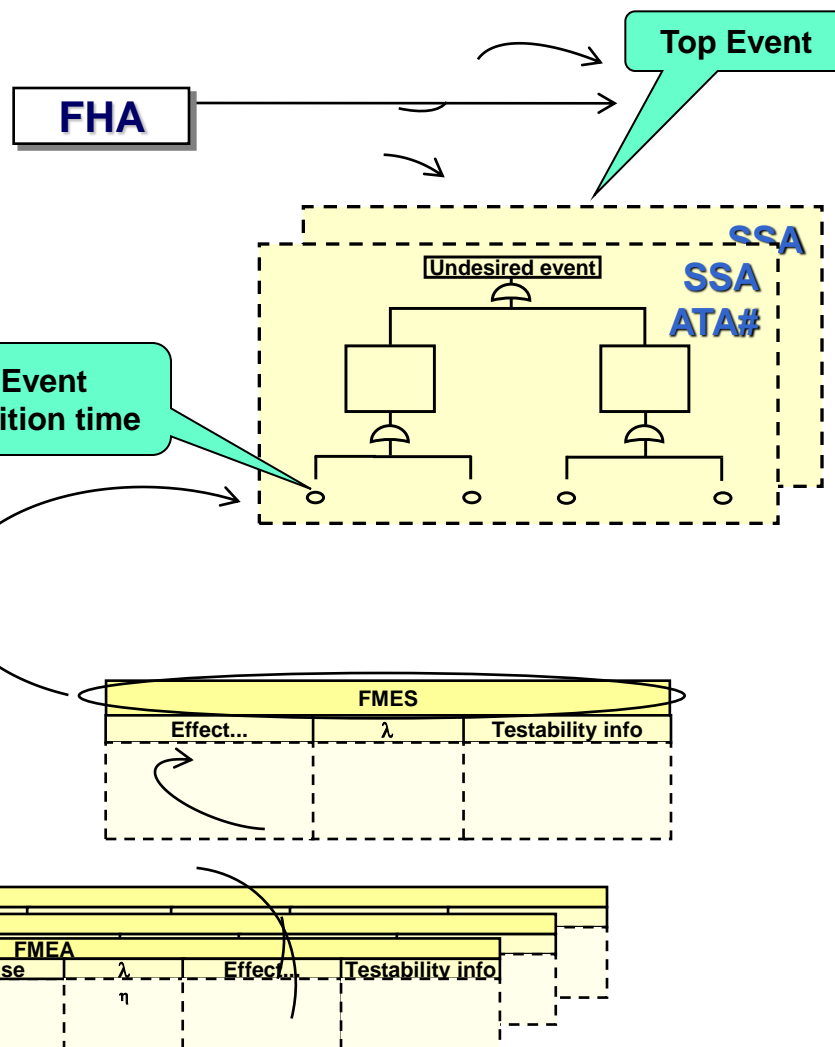
- Links with the other safety analyses

Functional Hazard Analysis (FHA)

**PSSA & SSA :
Fault Tree Analysis (FTA)**

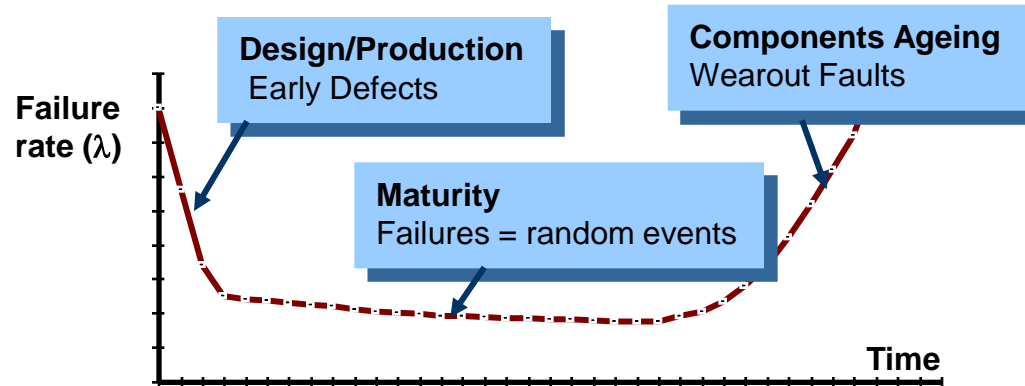
Failure Mode Effect Synthesis (FMES)

Failure Mode Effect Analysis (FMEA)

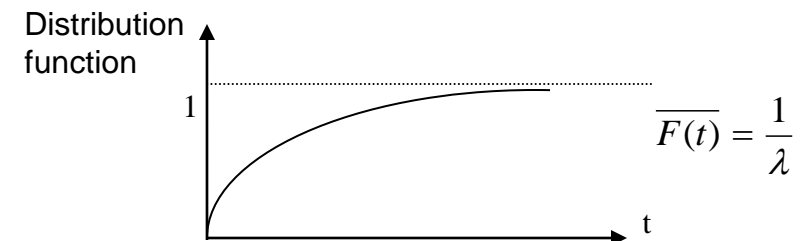


GEA Tianjin / 中国民航大学中欧航空工程师学院

- Failure rate = Number of failures / Observation Time
 - Experimental observations : the “bathtub curve”



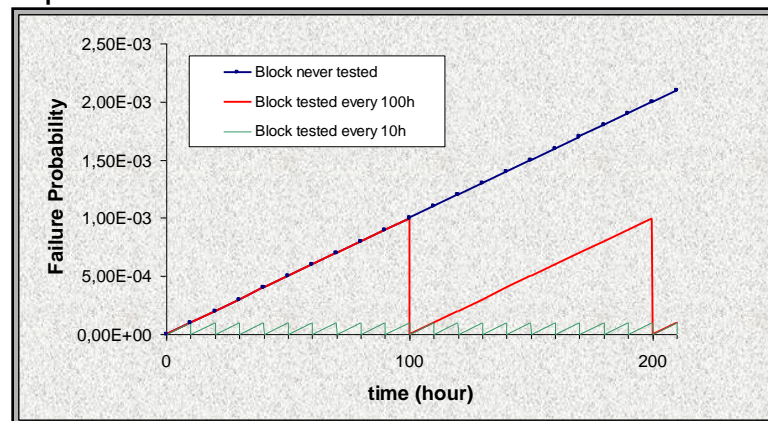
- Mathematical assumption : Useful life = maturity period → **Constant** failure rate
- Probability of failure at “time = t” predicted by Exponential law
 - $F(t) = 1 - e^{(-\lambda \cdot t)} \sim \lambda \cdot t$ when $\lambda \cdot t \leq 10^{-2}$



GEA Tianjin / 中国民航大学中欧航空工程师学院

Probabilities of failure and Times

- Notions of Exposure time, Active and hidden failures
 - The failure is susceptible to occur during **a certain time**
 - Active failure (ie detected during a flight) : $P \approx \lambda \cdot T_{\text{flight}}$
 - Hidden, dormant, latent failures
 - Are failures not detected during a flight
 - Dormant failures for life (never detected nor tested)
 - » Exposure time $T = \text{Aircraft life} \Rightarrow P \approx \lambda \cdot \text{AC life}$
 - Tested latent failures (*Power-on self tests, pre-flight tests, A/C checks*)
 - » Exposure time $T = \text{interval between 2 tests} \Rightarrow P \approx \lambda \cdot T$



GEA Tianjin / 中国民航大学中欧航空工程师学院

Equipment reliability (MTBF)



- Mean Time Between Failure : Several computations

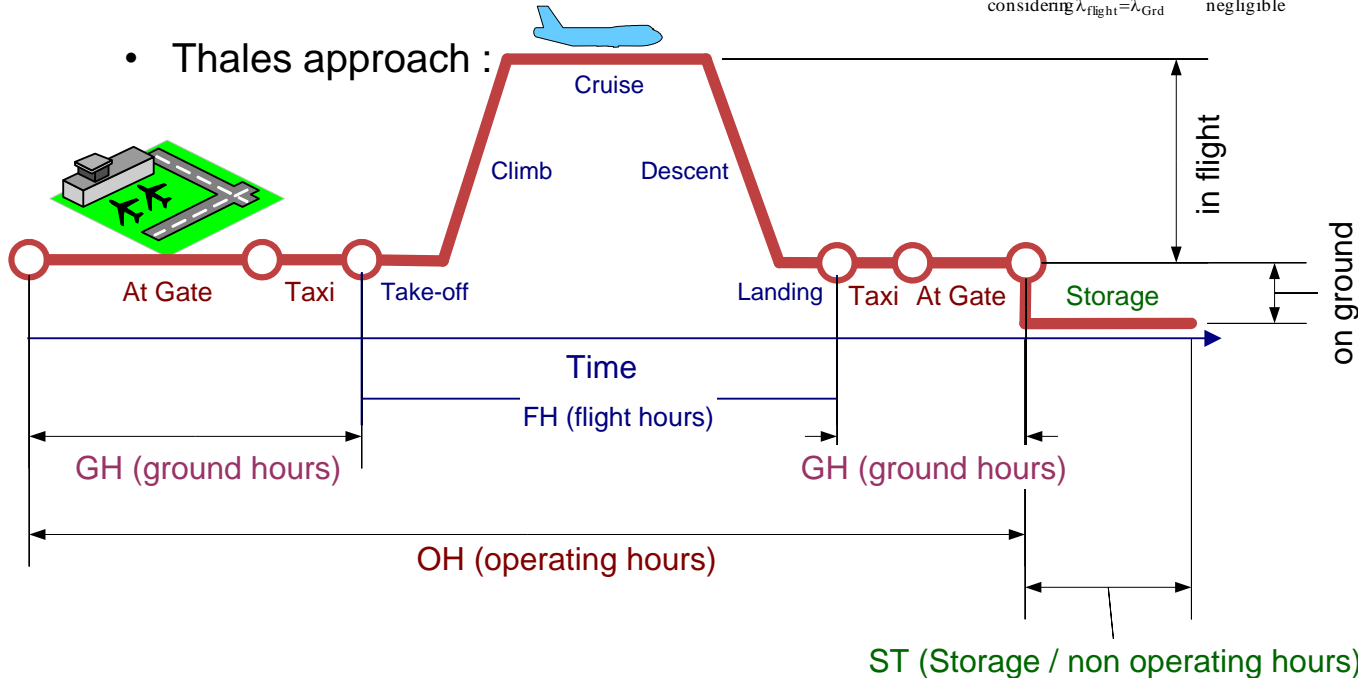
- MTBF = 1 / Failure rate (λ)
- Operational MTBF per FH prediction

$$MTBF_{(FH)} = \frac{1_{FH}}{\lambda} = \frac{T_{flight}}{\lambda_{flight} \times T_{flight} + \lambda_{Grd} \times T_{Grd} + \lambda_{St} \times T_{St}}$$

- General formula :

$$MTBF_{(FH)} = \frac{T_{flight}}{\underbrace{\lambda_{Grd} \times T_{OH}}_{\text{considering } \lambda_{flight} = \lambda_{Grd}} + \underbrace{\lambda_{St} \times T_{St}}_{\text{negligible}}} \cong \frac{T_{flight}}{T_{OH}} \times \frac{1}{\lambda_{Grd}}$$

- Thales approach :





GEA Tianjin / 中国民航大学中欧航空工程师学院

Part 3 – Assessment of systems safety

- Part 1 – Introduction to Safety concepts
- Part 2 – Avionics systems : design for safety
- Part 3 – Assessment of systems safety
 - Process guidelines
 - Dysfunctional analyses, Reliability
 - Development Assurance Level
- Conclusion

GEA Tianjin / 中国民航大学中欧航空工程师学院



❑ DAL is assigned using the [Safety Assessment Process](#).

❑ The DAL of a function or item depends on the [severity classification of Failure Conditions](#) in relation with this function or item (ARP4754 table 5-1)

Failure Condition Severity Classification	Top-Level Function DAL assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E



GEA Tianjin / 中国民航大学中欧航空工程师学院

Safety & System Architecture

- Part 1 - Introduction to Safety concepts
 - Generalities
 - Aircraft airworthiness
- Part 2 – Avionics systems : design for safety
 - Safe architectures
 - Candidate architecture assessment
- Part 3 – Assessment of systems safety
 - Process guidelines
 - Dysfunctional analyses, Reliability, DAL
- Conclusion

GEA Tianjin / 中国民航大学中欧航空工程师学院

How to ensure that a system is safe ?

Issue	Preventive means	Analyses	
Random hardware failure	Assessment of probability of scenario vs. its severity : - Equipment intrinsic reliability (MTBF) - Safe architecture (several channels)	FMEA, FTA	Safety
H/W or S/W systematic error	- Design dissimilarity - Equipment DAL / application of quality / V&V - Partitioning / segregation of critical functions	CMA, DAL allocation	
Human error induced by design	Ergonomy, AFM & maintenance procedures, etc.	HF study (prototyping , HEA ...)	Human Factor
Environment SEU	D0160E qualification, non-sensitive to SEU components, etc.	Tests	Qualif
Installation in aircraft, structure	- Aircraft zoning, segregation of critical paths - Safe-life, damage-tolerant design	ZHA, PRA	Safety



GEA Tianjin / 中国民航大学中欧航空工程师学院

Conclusion

- Safety is a key concept in the architecture design
 - Necessity to be addressed from the early beginning of projects
 - Identification of Safety performances of a product to contribute to its re-use in a different context or its evolutions
- Safety regulations evolve
 - Need of anticipation vs certification regulations
 - Need of constant improvement of products / systems
- A Tier1 is responsible of the safety of its system and of its integration within the aircraft
 - Need of lessons learnt from past in-service safety events



GEA Tianjin / 中国民航大学中欧航空工程师学院

Appendix 1 – Aviation internet sites

- More details on :
 - Statistics
 - <http://aviation-safety.net>
 - <http://www.flightsafety.org>
 - http://www.faa.gov/data_statistics/
 - Accidents / Incidents reports
 - <http://www.bea-fr.org/>
 - <http://www.nts.gov/aviation/aviation.htm>
 - ICAO Taxonomy
 - <http://www.intlaviationstandards.org/>

GEA Tianjin / 中国民航大学中欧航空工程师学院

Severity classification : Example

- Which severity for risks linked to Landing Gear ?
 - Annunciated inability to retract any Landing Gear ?
 - Annunciated loss of extension of any Landing Gear ?
 - Collapse of any Landing Gear :



• Nose L/G collapse ?

• Main L/G collapse ?





GEA Tianjin / 中国民航大学中欧航空工程师学院

Appendix 2 – zooms ... Quiz Landing Gear

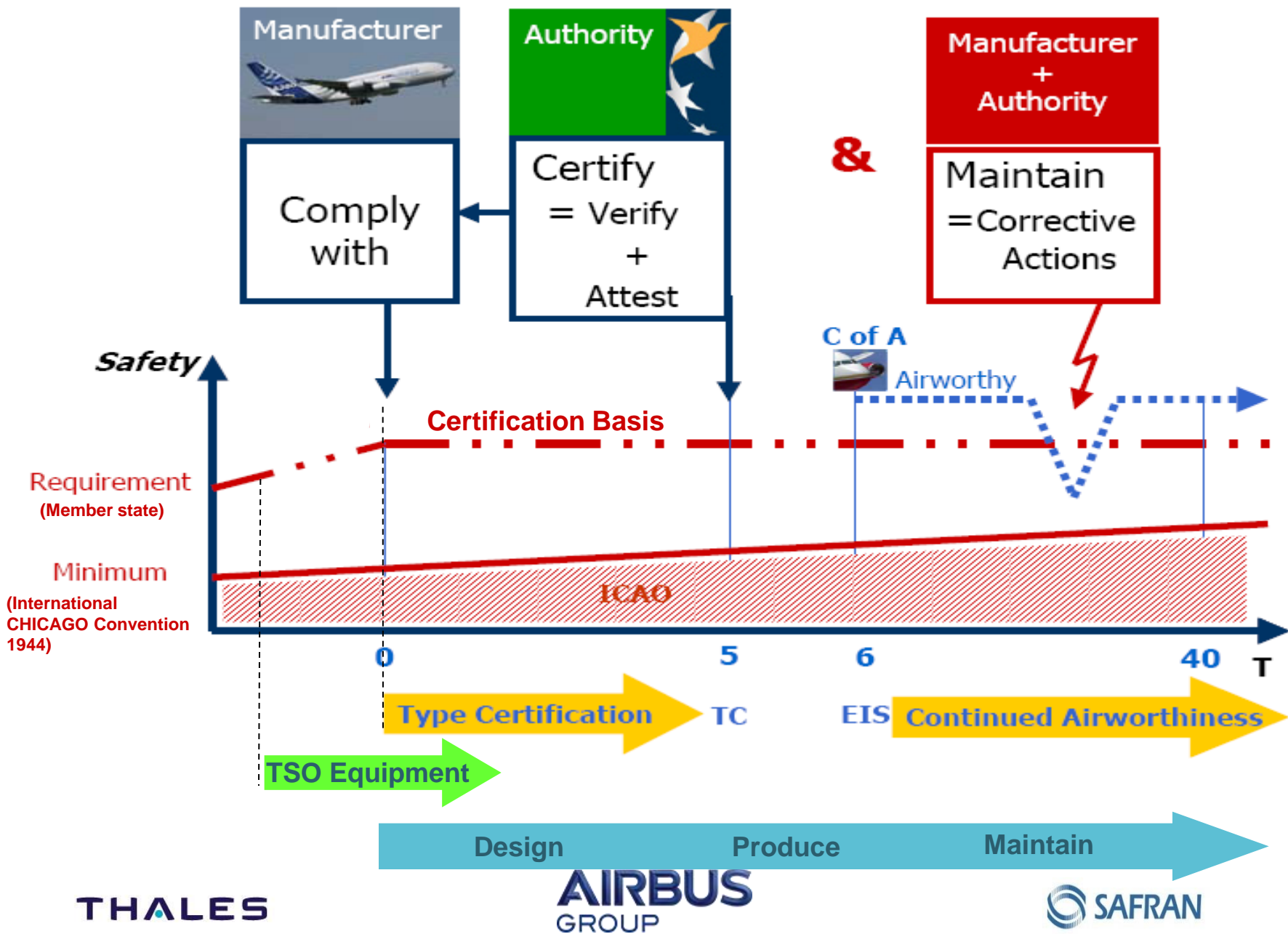
- Which severity for risks linked to Landing Gear ?
 - Annunciated inability to retract any Landing Gear ?
 - **MINOR** : In-Flight Turn Back + normal landing
 - Annunciated loss of extension of any Landing Gear ?
 - Nose Gear : **MAJOR** to **HAZARDOUS**
 - Main Gear : **HAZARDOUS** as A/C will have to perform a “Belly landing” (emergency procedure) and risk of damages of fuselage, passengers injuries. If loss of extension is not detected by crew, repercussions may be worse (HAZ to CAT).
 - Collapse of any Landing Gear
 - Nose Gear : **MAJOR** to **HAZARDOUS** as can lead to significant damages of fuselage but do not provoke A/C collapse
 - Main Gear : **HAZARDOUS** to **CATASTROPHIC**
 - If symmetrical collapse : potential runway overrun and A/C fuselage damages (HAZ)
 - If asymmetrical collapse, the risk is a potential veering off the runway and offside excursion, with a collapse of aircraft that may lead to wing rupture, fuel leakage and A/C fire (CAT)



GEA Tianjin / 中国民航大学中欧航空工程师学院

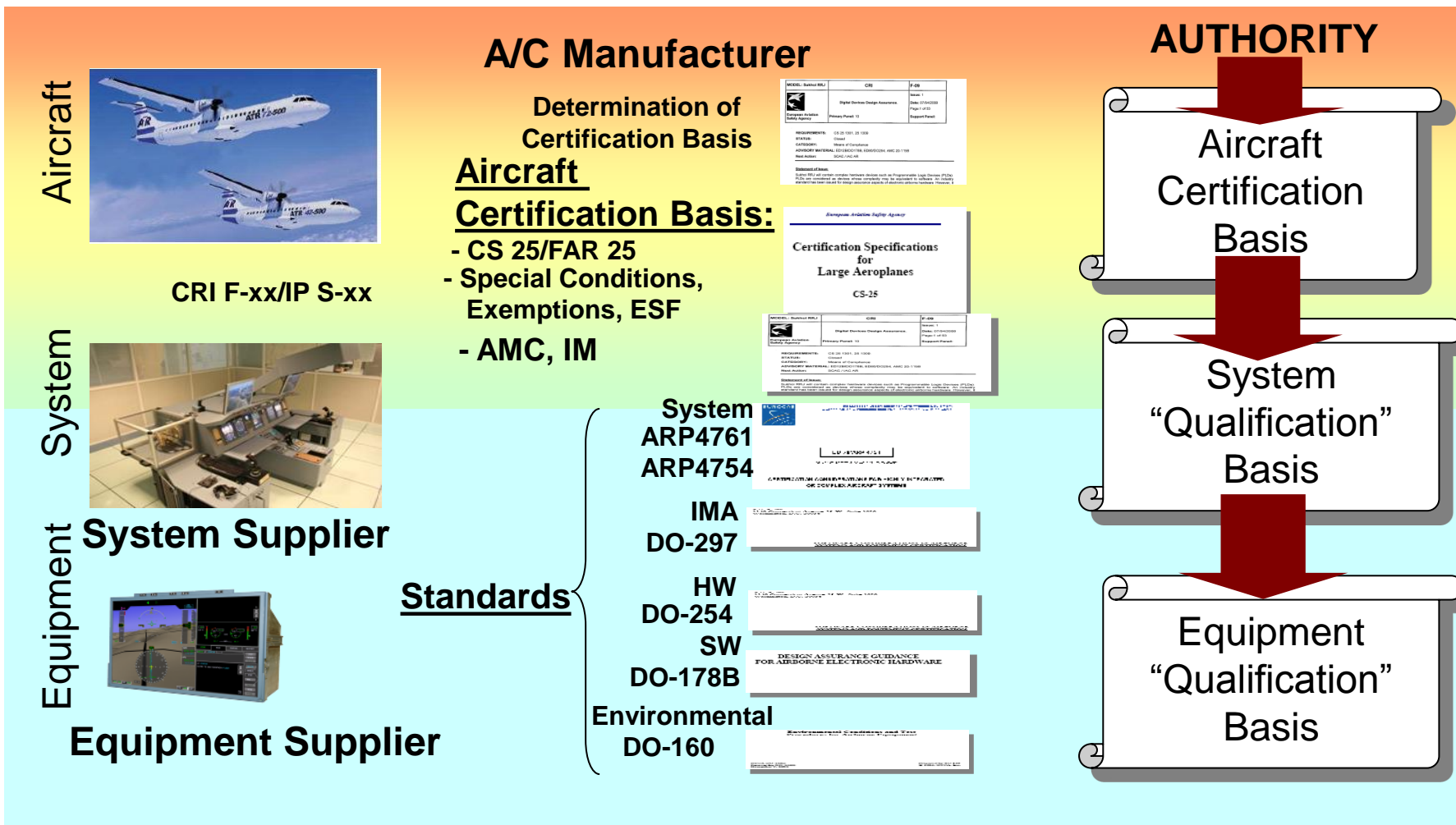
SB 503 - Avionics Technologies

1-2 Avionics Certification Process including applicable Standards



GEA Tianjin / 中国民航大学中欧航空工程师学院

Certification basis flow-down



GEA Tianjin / 中国民航大学中欧航空工程师学院

Acceptable
Means of Compliance

A/C Certification Basis
set of CS25/27/29 requirements

§ 1301 : Intended Function
§ 1309 : Failures



AMC 25.1309 / AC 20.174

Safety Assessment Process
Guidelines & Methods
(ARP 4761 / ED-135)

Aircraft & System Development
Processes
(ARP 4754 / ED-79)

Ensure that A/C functions
are correct, complete and safe

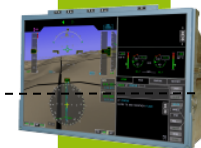
Aircraft



System



Equipment



Item /
Component



AMC 20-115 / CRI

Guidelines for Integrated
Modular Avionics
(DO-297/ED-124)

Electronic Hardware
Development Life-Cycle
(DO-254 / ED-80)

Software Development
Life-Cycle
(DO-178B/ED-12B)

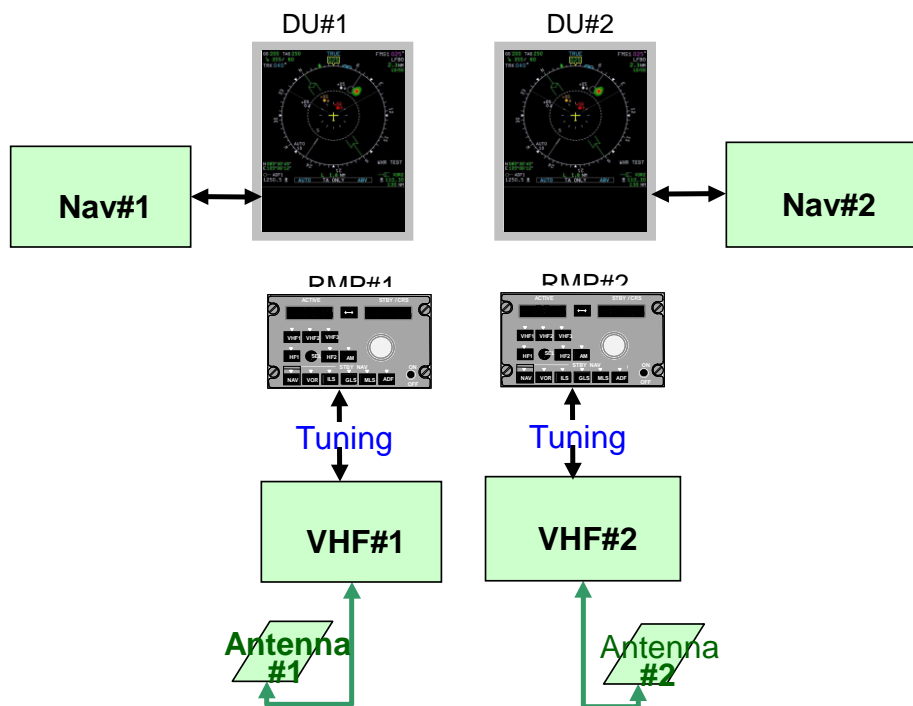
Ensure that SW and HW
are compliant to their
specifications

Like DO178 for SW and DO254 for HW, ARP4754-A is an Acceptable Mean of Compliance to ensure accurate Development Assurance Level for systems



GEA Tianjin / 中国民航大学中欧航空工程师学院

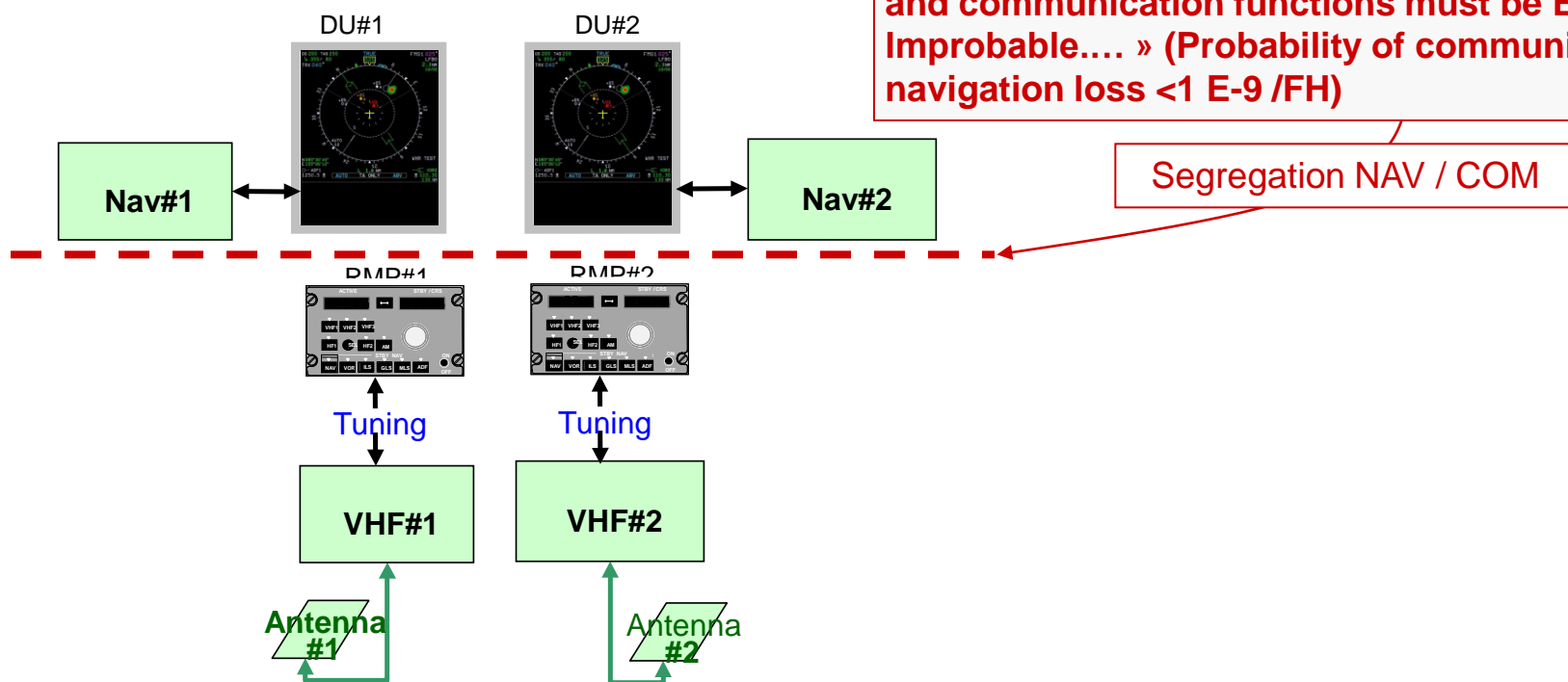
Example : 25.1307 Communication function



GEA Tianjin / 中国民航大学中欧航空工程师学院

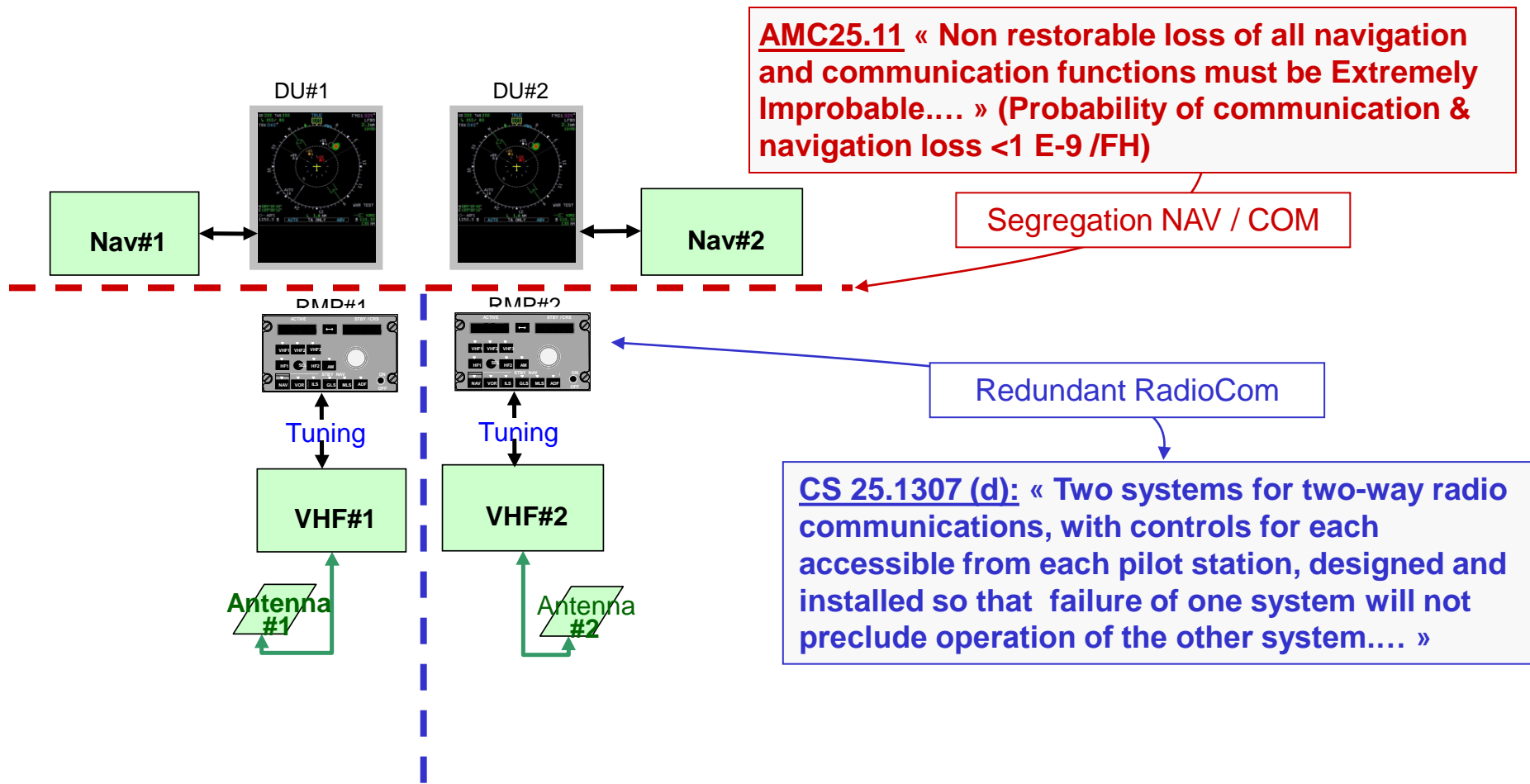
Example : 25.1307 Communication function

AMC25.11 « Non restorable loss of all navigation and communication functions must be Extremely Improbable.... » (Probability of communication & navigation loss $< 1 \text{ E-9 / FH}$)



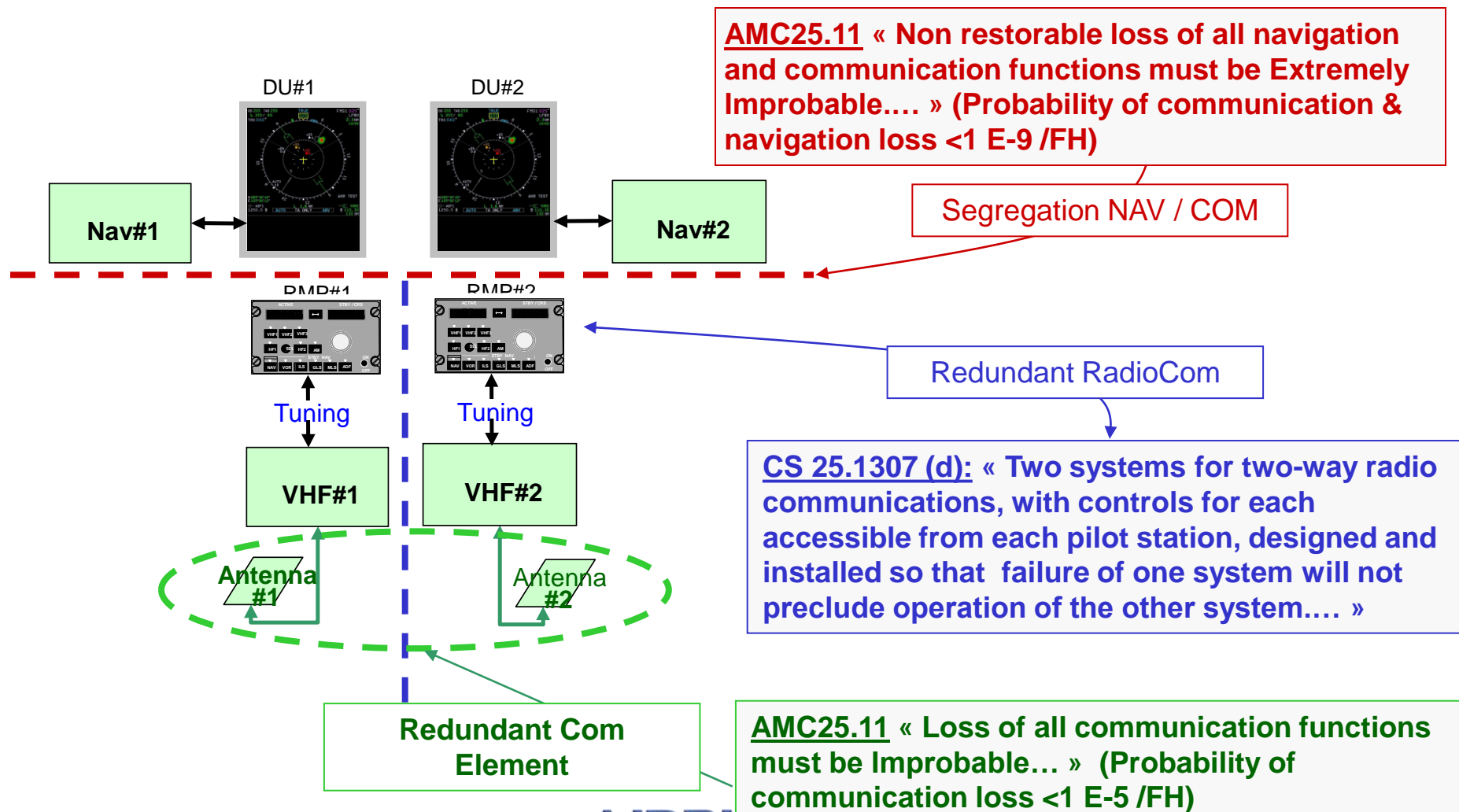
GEA Tianjin / 中国民航大学中欧航空工程师学院

Example : 25.1307 Communication function



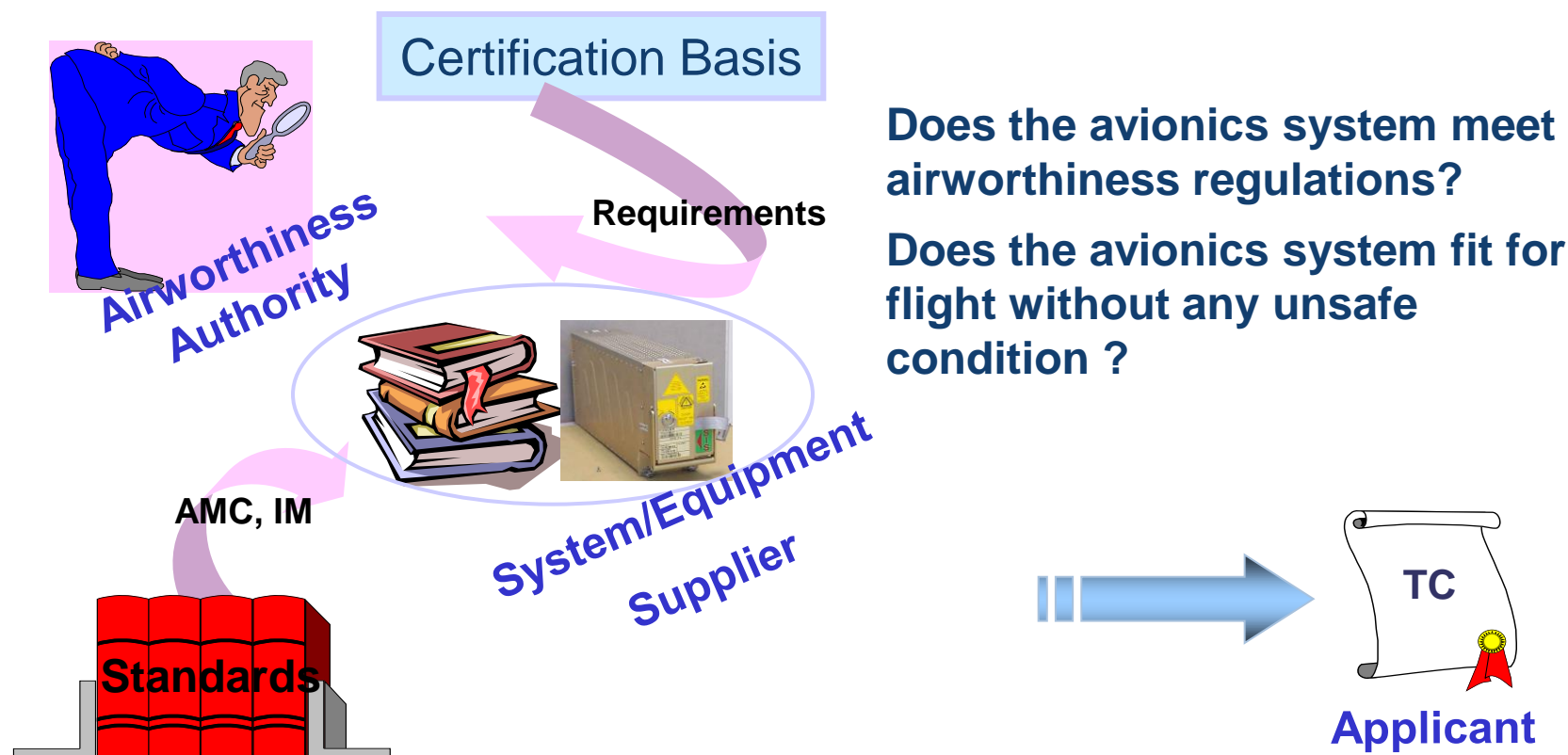
GEA Tianjin / 中国民航大学中欧航空工程师学院

Example : 25.1307 Communication function



GEA Tianjin / 中国民航大学中欧航空工程师学院

Airworthiness Authority Role and Involvement



AA involvement depends on the safety criticality of equipment, complexity of the development, certification experience, service history, novelties

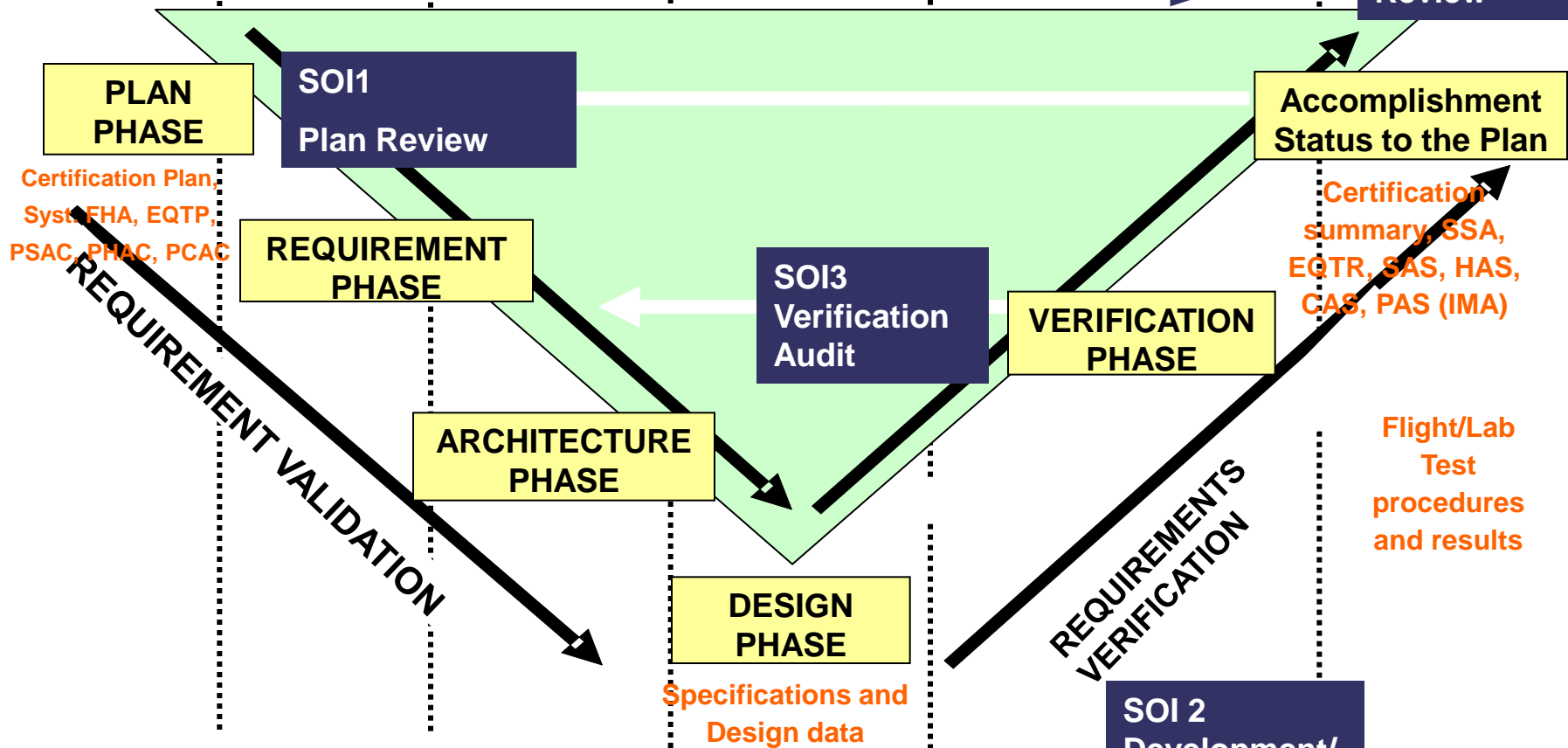
GEA Tianjin / 中国民航大学中欧航空工程师学院

V Development Cycle

Manufacturer requirements
Certification basis

SYSTEM / SUB-SYSTEM / EQUIPMENT Development cycle

SOI4
Certification
Review



SOI : Airworthiness Authority « Stage Of Involvement »

GEA Tianjin / 中国民航大学中欧航空工程师学院

Appendix 4 – Glossary and Definitions

DEPENDABILITY ACTIVITIES

- **Dependability.** Generic concept as the ability to deliver service that can justifiably be trusted. Dependability encompasses four properties, leading to the acronym RAMS, often used as an equivalent to “dependability” :
 - *Reliability* (continuity of correct service);
 - *Availability* (readiness for correct service);
 - *Maintainability* (ability to undergo modifications and repairs);
 - *Safety* (Absence of catastrophic consequences on the human and the environment).
- **Testability.** The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met.
- **Security.** Ability to avoid illegal access to service and information.
- **Dependability engineering.** Validation which consists in ensuring the required dependability properties taking into account the possible threats which are failures, errors and faults.
- **Certification.** Legal recognition by the certification authority that a product, service, organisation or person complies with the requirements.

SYSTEM DESIGN

- **System.** A combination of components, parts, and elements, which are inter-connected to perform one or more functions.
- **Complex system (AMC25.1309 / DO254).** A system is Complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or deterministic tests.
- **Conventional system.** A system is considered to be Conventional if its functionality, the technological means used to implement its functionality, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly-used.

SYSTEM DEVELOPMENT

- **Development Assurance.** All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.
- **Development Assurance Levels (DAL).** Ranking of the severity of an item which is transferred from the Failure Condition severity levels to the entities whose failures can cause or contribute to the considered Failure conditions. The terminologies Safety Integrity Levels (SIL) or (for software) Software Criticality (ranking of a piece of software based on the severity of its potential failures) may be also used.

FAILURE CONDITION, EVENTS ...

- **Failure Condition (AMC25.1309).** A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events. the terminologies *feared event* or *undesired event* are also used.
- **Failure Condition severity.** Ranking of the negative consequences of undesired events.
- **Event.** An occurrence which has its origin distinct from the aeroplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage.

GEA Tianjin / 中国民航大学中欧航空工程师学院

SYSTEM STATES & BEHAVIOR

Appendix 4 – Glossary and Definitions

- *Failed, Faulty, Degraded, Erroneous behavior, Error.* State of a system or component after the occurrence of a failure, an error, or a fault.
- *Degraded mode.* The detection of a failure of a module leads to a controlled change of its behavior. The modules functionality is reduced, conforming to a reduced or lowered set of requirements.
- *Fail stop.* Property of a system (subsystem, equipment) such that its failures lead to a situation where the service is halted.
- *Fail safe.* Property of a system (subsystem, equipment) such that its failures lead to a known state and within acceptable margins of “safe” situation.
- *Fail operational.* Property of a system (subsystem, equipment) such that its failures lead to a safe situation and in operational (working) state.
- *Fault Tolerance.* Means to avoid failed or faulty states of the system in the presence of failures. Forms of fault tolerance may reach, in case of fault, either a full operational state of the system or a degraded mode.

FAILURES, FAULTS, ERRORS ...

- *Error.* An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation.
- *Fault.* Hypothesized or adjudged cause of an error. Mainly used for Hardware or Software design errors.
- *Failure.* An occurrence, which affects the operation of a component, part, or element such that it can no longer function as intended, (this includes both loss of function and malfunction). Note: Errors may cause Failures, but are not considered to be Failures.
- *Failure mode :* Characterization of the way a product fails.
- *Permanent, intermittent or transient.* Temporal characteristics of a failure or an error.

REDUNDANCY

- *Redundancy.* The presence of more than one independent means for accomplishing a given function or flight operation to be fault tolerant against failures of some of the means.
- *Active redundancy.* Fault tolerant architecture where all redundant elements process the inputs but only one actually provides the output.
- *Passive redundancy:* Fault tolerant architecture where only one of the redundant elements processes the inputs.
- *N-Modular redundancy:* Fault tolerant architecture with N redundant elements which all provide the outputs to a voting mechanism.

MONITORING, TESTABILITY

- *FDIR (Failure Detection, Isolation and Recovery).* Fault tolerance techniques involving the explicit detection of abnormal situations, followed by the handling of errors and faults up to the passivation.
- *Monitoring.* Test procedure, observing certain functions or (data-) objects at runtime.
- *Fault compensation.* Fault tolerance techniques without explicit detection of the faulty item.
- *Passivation.* Fault tolerance techniques dealing with the deactivation of a faulty module, after detection of its failure(s). Its behavior has no more impact on the rest of the system.
- *Test.* A test verifies the correct work of a system, equipment, board, hardware block or of a functional block. A test may be run off-line or on-line, according to what is called the test activation time (defines, when a test is performed). Various detection mechanisms and techniques exist : plausibility checks, error detection codes, data and control flow monitoring ...
- *Built-in tests (BIT).* Part of the system, which controls the monitoring and diagnosis activities. BIT can be activated continuously, cyclically or at power up (also called in that case *power on self tests*).

GEA Tianjin / 中国民航大学中欧航空工程师学院

Appendix 4 – Glossary and Definitions

INDEPENDENCE and SEGREGATION

- *Independence*. Characteristic of a set of redundant or command/monitor channels, protecting them against common cause faults.
- *Diversity*. Special form of redundancy, where objects with different characteristics are used to minimize common cause failures due to development faults.
- *Partitioning*. Separation of subsystems, to ensure that they do not influence each other. For software modules running on one processor this implies the separation of memory and a strict scheduling (temporal and spatial partitioning).

RELIABILITY, FAILURES RATE, MTBF ...

- *Failure rate*. The probability of failure per unit of time of items in operation; sometimes estimated as a ratio of the number of failures to the accumulated operating time for the items. Note : an occurrence rate may be associated specifically to the various modes of a failure; this is noted “%failure rate” (Part of the failure rate associated with one failure mode by ratio of the total failure rate).
- *Reliability*. The probability that an item will perform its intended function for a specified interval under stated conditions.
- *Reliability Growth*. The improvement in reliability caused by the successful correction of deficiencies in an item design or manufacture.
- *Derating*. Using an item in a way that applied stresses are below rated values.
- *MTBF (Mean Time Between Failure)*. The average time during which all parts of the item perform its intended function within their specified limits, during a particular measurement period under stated conditions.
- *MTTF (Mean Time To Failure)*. The average failure free operating time, during a particular measurement period under stated conditions. Basic measure of MTBF for no repairable systems.
- *MTTR (Mean Time To Repair)*. The average time for corrective maintenance actions. Typically includes fault isolation, remove and replacement of failed item(s) and checkout.
- *MTBCF (Mean Time Between Critical Failures)*. The average time between failures which cause a loss of a system function defined as “critical” by the customer
- *MTBUR (Mean Time Between Unscheduled Removal)*. The average time between all maintenance actions requiring removal and replacement of a box or subsystem.

ACTIVE / DORMANT FAILURES AND CCMR

- *Active Failure*. Failure which leads directly to a faulty state, detected or not, of a system.
- *Latent Failure*. Failure which is not detected and brought to the flight crew awareness, and which would not directly lead to a faulty state of a system unless combined with other active failures. A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one, which would in combination with one or more specific failures, or events result in a Hazardous or Catastrophic Failure Condition.
- *Check*. An examination (e.g., an inspection or test) to determine the physical integrity and/or functional capability of an item. Also called “preventive maintenance”.
- *Candidate Certification Maintenance Requirements (CCMR) & Certification Maintenance Requirements (CMR) - (AMC25.1309)*. Check (periodic maintenance or flight crew check) which cannot be accepted as basic servicing or airmanship and may be used in a safety analysis to help demonstrate compliance with CS 25.1309(b) for Hazardous and Catastrophic Failure Conditions. AMC 25.19 defines a method by which Certification Maintenance Requirements (CMRs) are identified from the candidates. A CMR becomes a required periodic maintenance check identified as an operating limitation of the type certificate for the aeroplane.

GEA Tianjin / 中国民航大学中欧航空工程师学院

Appendix 4 – Glossary and Definitions

FLIGHT OPERATIONS – HUMAN FACTORS

- **CRM.** Crew Resource Management. CRM encompasses a wide range of knowledge, skills and attitudes including communications, situational awareness, problem solving, decision making, and teamwork; together with all the attendant sub-disciplines which each of these areas entails. CRM can therefore be defined as a management system which makes optimum use of all available resources - equipment, procedures and people - to promote safety and enhance the efficiency of flight operations. CRM training for crew are defined in AC 120-51.
- **SOP.** *Standard Operating Procedure.* SOPs should identify and describe the standard tasks and duties of flight-crew for each flight phase (i.e., what-to-do and when-to-do). SOPs should be accomplished by recall but critical tasks (e.g., selections of systems and changes of aircraft configuration) should be cross-checked by use of normal checklists (i.e., for error detection and correction), according to the phase of flight. SOPs should be supplemented by information on specific operating techniques (e.g., adverse weather operation) and by operational recommendations for specific types of operations (e.g., operation on wet or contaminated runway, operation in ETOPS area and/or in RVSM airspace). SOPs should assume that all aircraft systems operate normally and that all automatic functions are used normally. The FAA defines the scope and contents of SOPs in Advisory Circular (AC) 120-71.
- **AFM.** *Airplane Flight Manual.* The Aircraft Flight Manual (AFM) is a book containing the information and instructions required to operate the aircraft safely. The pilot must comply with this AFM information. A typical AFM will contain the following : **1/ Limitations** - the 'envelope' of maximum speeds; maximum weights; allowable centre of gravity range; maximum engine RPM, temperatures and oil pressures, etc; and allowable manoeuvres and other limits, within which the aircraft must be operated to be safe. **2/ Operating procedures** - aircraft procedures, speeds and configurations used to achieve expected performance and behaviour in Normal situations, and achieve safe outcomes in some specified Abnormal or Emergency situations (such as a forced landing after engine failure). **3/ Performance** - the required variation of the aircraft's maximum allowable weights, as affected by air pressure and temperature, in order to Take-off or land in available runway distance, Climb at the minimum required gradient, or greater gradient needed to clear obstacles in the intended flight path following take-off or missed approach. **4/ Other information and instructions** necessary to safely operate the aircraft. The AFM is as important as any other critical part of the aircraft. It is a part of the type design.
- **QRH.** *Quick Reference Handbook.* A Quick Reference Handbook (QRH) is a handbook containing extracts from the Aeroplane Flight Manual (AFM) which may need to be referred to quickly and/or frequently, usually including Emergency and Abnormal procedures. The procedures may be abbreviated for ease of reference (although they must reflect the procedures contained in the AFM). Two copies of the QRH must be provided on the flight deck so that both pilots have access to a copy.
- **FCOM.** *Flight Crew Operating Manual.* A FCOM is a technical publication written for a specific aircraft which is used by flight crew members to operate that aircraft and to explain the technical specifications for that aircraft. It contains for example : system descriptions, Limitations, QRH procedures with comments (normals, following failures (abnormal), emergency), techniques, performances (simplified compared with AFM), systems operations, OEB (operations engineering bulletins), ...



GEA Tianjin / 中国民航大学中欧航空工程师学院

Appendix 4 – Glossary and Definitions

ICAO [accident / incident] OCCURRENCE CATEGORY ABBREVIATIONS

ARC	Abnormal Runway Contact
AMAN	Abrupt Maneuver
ADRM	Aerodrome
ATM	Air Traffic Management
CABIN	Cabin Safety Events
CFIT	Controlled Flight into or Toward Terrain
EVAC	Evacuation
F-NI	Fire/Smoke (Non-Impact)
F-POST	Fire/Smoke (Post-Impact)
FUEL	Fuel Related
GCOL	Ground Collision
RAMP	Ground Handling
ICE	Icing
LOC-G	Loss of Control – Ground
LOC-I	Loss of Control – Inflight
LALT	Low Altitude Operations
MAC	Loss of Separation / Near Midair Collisions / Midair Collision / TCAS Alert
OTHR	Other
RE	Runway Excursion
RI-A	Runway Incursion – Animal
RI-VAP	Runway Incursion – Vehicle, Aircraft or Person
SEC	Security Related
SCF-NP	System/Component Failure or Malfunction (Non-Powerplant)
SCF-PP	System/Component Failure or Malfunction (Powerplant)
TURB	Turbulence Encounter
WSTRW	Windshear or Thunderstorm
USOS	Undershoot/Overshoot
UNK	Unknown or Undetermined

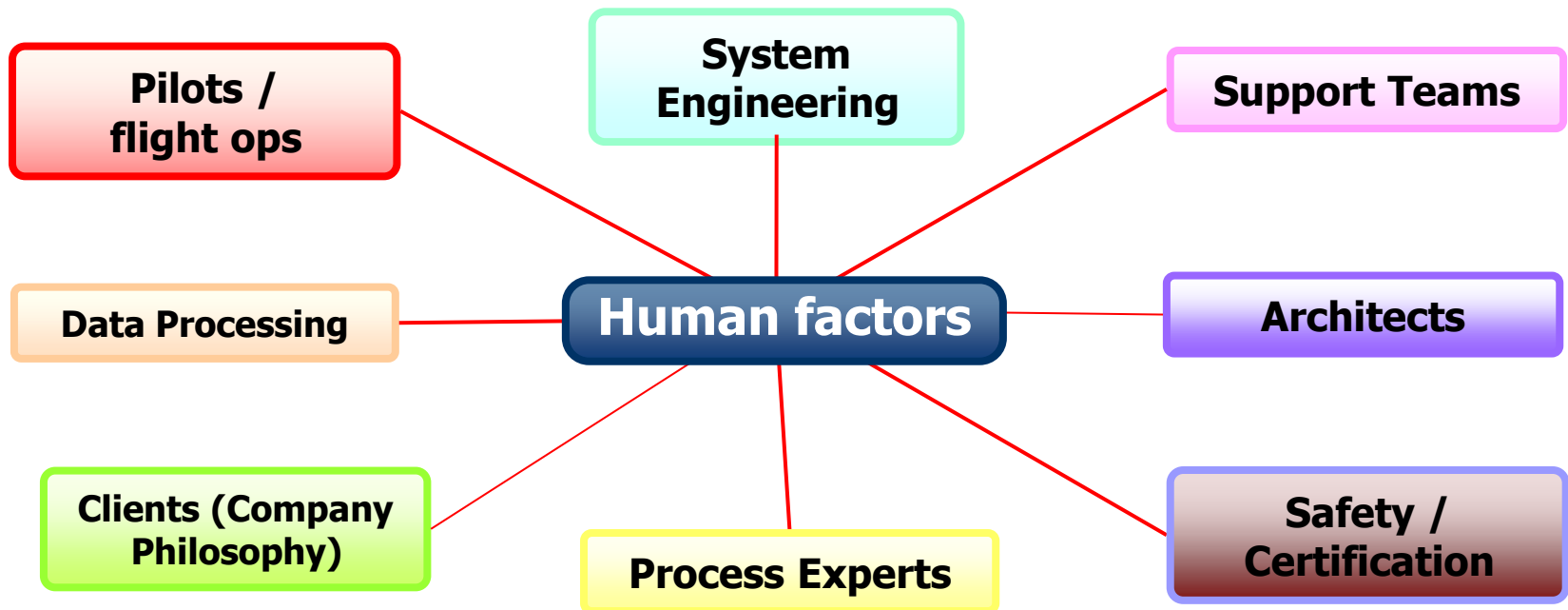


GEA Tianjin / 中国民航大学中欧航空工程师学院

SB 503 - Avionics Technologies 1-3 Human factors

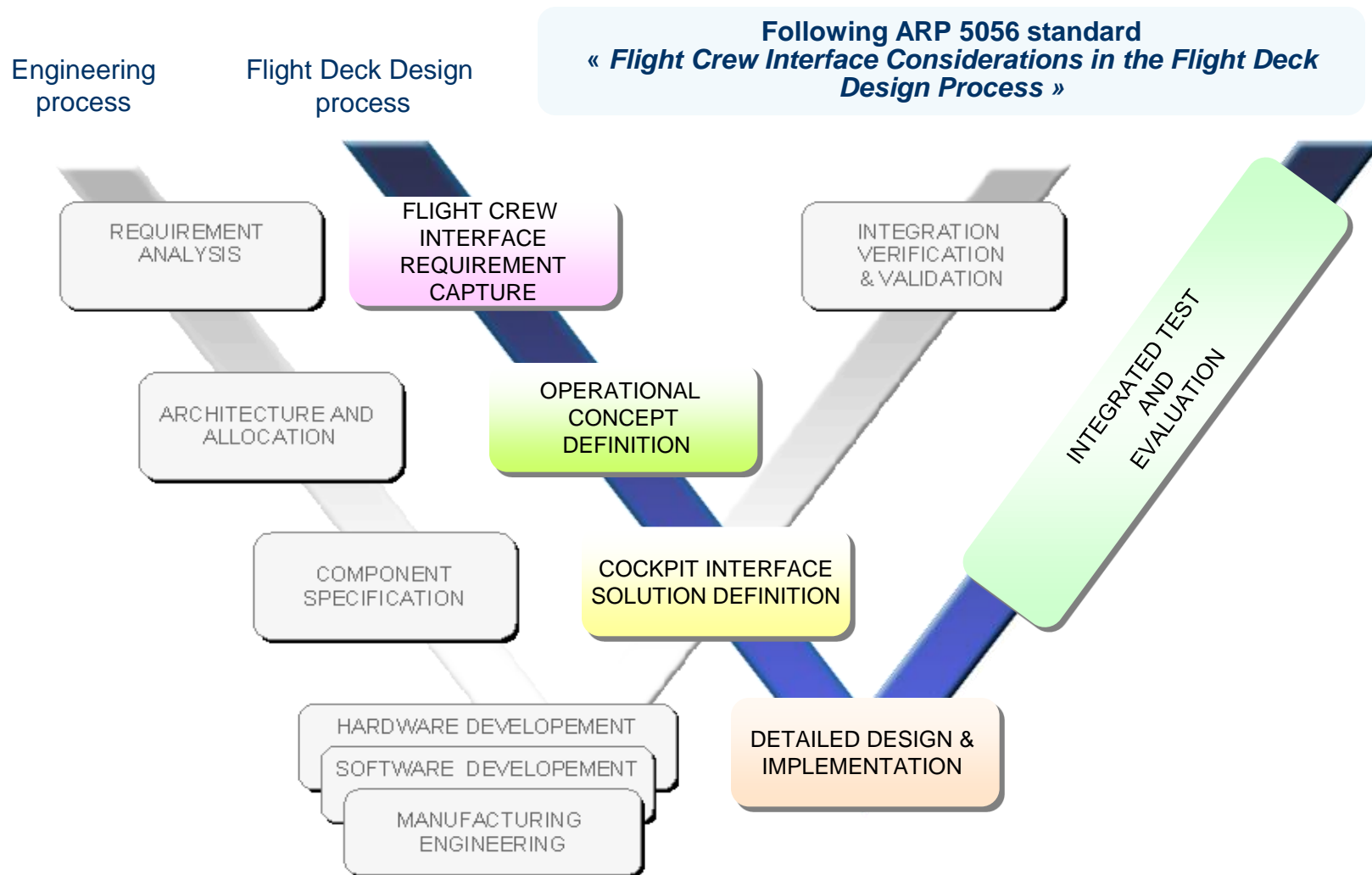
GEA Tianjin / 中国民航大学中欧航空工程师学院

Human Factors: The Actors



To stand right in the Middle of the Concepts team

GEA Tianjin / 中国民航大学中欧航空工程师学院



GEA Tianjin / 中国民航大学中欧航空工程师学院

Methodology HF & Tools

