Agenda (2/3)

- Module 4 – Design requirements and Safety process
  - 4-1 Requirements
  - **4-2 Safety process**
- Module 5 – Aircraft power systems
  - 5-1 Hydraulic power systems
  - 5-2 Electric power systems
- Module 6 – Aircraft Control systems Architectures
  - 6-1 Hydro Mechanical Systems
  - 6-2 Fly by wire systems
  - 6-3 Fly by wire systems new generation
  - 6-4 A320 FAL Visit

General

- This presentation will describe the way how safety is adequately addressed in the aircraft design (with focus on system design)
- A popular definition of safety is:
  - Minimum safety level is achieved when the aircraft design is in compliance with the airworthiness rules and regulations.

- Therefore , the following is mainly oriented on the regulatory framework and the advisory material existing on the subject.

Agenda

- The safety process
- System design for safety
- Safety assessment methodes

General

- Safety is the top priority everywhere in all areas of the aviation industry
- Due to the global efforts spend during the last decades on industry and governmental side safety level has drastically improved. Major contributors were :
  - Technical standards have evolved (technologies, materials, design tools, manufacturing methods, quality standards,)
  - Governmental guidance and rulemaking have evolved
  - International cooperation programs (ICAO guided,)
    - Airworthiness Rule harmonization effort (FAR25, CS 25, CAAC part 25..)
  - Continuous Communication (conferences, dialog on issues ….) between all stakeholders (regulatory body's, aircraft manufacturer, supplier, aircraft operator, maintenance organisations, Airports , Air traffic control)

General

- Standisation by industry organisations
  - SAE, RTCA, Eurocae, ….

General

- The improvement is visible:
- The annual accident rate (number of accident / 1 million flight hours)has decreased from 1960 to today by a factor of more than 100. The current figure is stable at this (low) value since a number of years and count actually 0.15 despite the fact of a significant increase of commercial aviation.
- Aircraft accidents are always cause by several factors ranging from:
  - Flight crew error 55%
  - Weather 13%
  - Aircraft structure and systems 17%
    - The systems contribution is 10%

Safety and Regulation

- Continuously there has been an increase on the degree of system complexity and integration and also in the number of safety critical functions performed by aircraft systems.

- In order to address the hazards that could result from failures of aircraft systems and the interaction between them, the use of a very structured means for the design process to finally show compliance to the requirements is necessary.

Safety and Regulation (2)

- The airworthiness authorities have addressed that in the recent issues of the FAR25 respective CS25 with paragraph 25.1309
- 25.1309b (and the relevant guidance material) specifies required safety level for the systems design in qualitative terms.
  - It requires that a safety assessment be made.
  - Assessment techniques are proposed to determine the (inverse) relationship between the probability and the severity of each failure condition
  - Use of service experience data of similar previously approved systems is allowed
  - Demonstration thorough qualitative analysis

Standardization/harmonization at Industry level

- Also the Industry has made efforts to issue guidance material for the design and certification of highly integrated and complex systems. SAE issued:
  - ARP 4761 (covered by ED-135)
    - Safety assessment process und guideline
  - ARP 4754 (covered by ED-79 from Eurocae)
    - System development process
  - ARP 5150/5151
    - Safety assessment of aircraft in commercial service
- The use of this standards is accepted by the AA as means of compliance to the 25.1309 requirement

Wording of 25.1309b

- (b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that
  - (1) Any catastrophic failure condition
    - (i)is extremely improbable; and
    - (ii) does not result from a single failure; and
  - (2) Any hazardous failure condition is extremely remote; and
  - (3) Any major failure condition is remote.

In other words: the severity of a failure (major/hazardous or catastrophic) will be linked with the probability (remote , extremely remote, improbable…) for the risk assessment

Risk assessment matrix

Severity Classification	FAA / EASA	Minor	Major	Severe Major / Hazardous	Catastrophic
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 (passengers - cabin crew)	*Some physical discomfort*	*Physical distress, possibly including injuries*	*Serious or fatal injury to a relatively small number*	*Multiple fatalities*

Severity Classification	FAA / EASA	Minor	Major	Severe Major / Hazardous	Catastrophic
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

Wording of 25.1309C

- (c) Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action. A warning indication must be provided if immediate corrective action is required. Systems and controls, including indications and annunciations must be designed to minimize crew errors, which could create additional hazards.

Wording of 25.1309d

- Electrical wiring interconnection systems must be assessed in accordance with the requirements of CS 25.1709.

Agenda

- The safety process
- System design for safety
- Safety assessment methodes

The design process basics

Design for minimum risk.

Design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection.

Incorporate safety devices.

If identified risks cannot be eliminated through design selection, reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.

The design process basics

Provide warning devices.

When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response. Warning signs and placards shall be provided to alert operational and support personnel of such risks as exposure to high voltage and heavy objects.

Develop procedures and training.

Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic, hazardous, major, or critical severity.

How to design for safety?

- Failure causes and type of failure (passive, operational) need to be identified and the consequences of the failure needs to be analyzed
- Any potential failure must be analyzed regarding the failure effect
  - System malfunction
  - System loss
  - The cascade of potential failure combinations must be established
- Compensation means must be invented to eliminate the failure case or minimize the consequences to the individual component and to the overall aircraft

Design principals/techniques to ensure safe design

- Design integrity and quality, including life limits, to ensure intended function and prevent failures
- Redundancy or back up System to enable continued function after any single failures (flight control, hydraulic system, electrical power….)
- Isolation/independence of Systems, components and elements so that a failure of one does not cause the failure of an other.
- Proven reliability so that multiple, independent failures are unlikely to occur at the same flight
- Failure warning or/and indication to provide detection
- Flight crew procedures for use after failure detection, to enable continued safe flight and landing by specific crew action
- Checkability, the capability to check components condition

Means for safe design summary

- Means for Safe design
  - Simplex, Duplex, Triplex Quadruplex design
  - Monitoring and voting
  - Warning and indication
  - Independence, physical separation
  - Life limits
  - Check procedure, automatic or Maintenance (CMR's)
  - Restricted use (MEL)
  - Training of pilots and maintenance staff

How to design for safety?

This is an iterative process which starts right at the beginning of the indicial design, (more than 5 years before first flight)

The potential hazardous/catastrophic failures and the related failure cascade lead to the early design decisions on the architecture of the aircraft and the related systems /equipment

Initial failure probabilities will be taken from the design experience and in service reliable information's.

Design tools are used to manage complex failure combinations.

How to design for safety?

- In sequence:
- FHA on aircraft level
- Definition of the safety objectives for each component/ system/equipment
- Preliminary System safety analysis
- Continuous update of SSA during the design process in full coordination with the design process of the full AC. (“other SSAs). Formal check points established (definition freezes, design freeze, start production, start labtesting first flight, certification)

Agenda

- The safety process
- System design for safety
- Safety assessment methodes

Acceptable techniques for safety assessment and compliance demonstration

- FHA; Functional hazard assessment to identify and classify potential hazardous failure conditions and to describe them in functional terms
- Analysis of failure condition,
  - Minor (failure condition may be probable)
  - Major (failure condition must be improbable)
  - Catastrophic (failure condition must be shown extremely improbable)
- Consider Operational or environmental conditions
  - Statistical derived probability are accepted
- Latent failures ,
  - CMR's could help

Acceptable means of compliance

- Acceptable means of compliance require that warning information must be provided to alert the crew to unsafe system operating conditions and to enable them to take appropriate corrective action
  - Failure warning my be natural or designed in the system
  - Procedures (if needed) for the crew follow up should be described in the Aircraft flight manual
  - Even if operational performance is not directly affected warning is required if it is necessary for the crew to take precautions (reduction of safety margins)
  - CMR's are not allowed a replacement of warnings
  - Appropriate arrangement of switches and control devices relative to each other are requested to avoid incorrect crew action (guarded switches)

Qualitative assessment

- Methods used for assessing the cause, severity and likelihood of failure condition
  - Design appraisal
  - Installation appraisal
  - Failure mode and effect analysis
  - Fault tree or reliability block diagram analysis
  - Qualitative probability terms
    - Probable : occurrence more than one times during the operational life of the airplane
    - Improbable: not anticipated to occur during the operational life of the airplane but may occur occasionally during the entire operational life of all airplanes of one type
    - Extremely improbable , conditions so unlikely to not occur during the entire life of all aircraft of one typ.

Quantitative assessment

- A quantitative analysis may be used to support experienced engineering and operational judgment and to support the qualitative analysis.
  - Probability analysis
    - Base on engineering judgment and in service experience and acceptable industries standards
    - Take margins
  - Quantitative probability terms are:
    - Probable , greater than 1x 10 minus 5
    - Imporobable, 1x10 minus5 or less but greater than 1x10 minus 9
    - Ectremly improbable, 1x10minus 9 or less

Operational and maintenance considerations

- Flight crew action,
  - Credit may be taken from correct and appropriate flight crew action
  - Credit may be taken from flight crew performance of CMR's
  - Approved AFM
- Ground crew action
  - Credit may be taken from accomplishment of of reasonable CMR's
  - Approved AMM
- Flight with equipment inoperative
  - Is allowed , A list of equipment and functions which do not need to be operative for safe flight and landing stating the compensating precautions that should be taken must be developed (operational and time limitations, ground or flight crew checks)
  - Approuved MMEL

Guidelines and methods for conducting safety assessment process ARP4761

- Functional Hazard Assessment (FHA)
- Fault Tree Analysis(FTA)
- Failure mode and Effects Analysis(FMEA)
- Failure Modes and Effects Summary (FMES)
- Common Cause Analysis (CCA)
- Zonal Safety Analysis (ZSA)
- Particular Risks Analysis (PRA)
- Common Mode Analysis (CMA)

The continued airworthiness process

- Even if the aircraft is ones certified (and considered as safe) the aircraft manufacturer design organization must continuously monitor the in service operation of the fleet and prove -case by case- the the design assumptions.
- A monitoring system is in place, Airline and AA report events to the aircraft manufacturer.
- Analysis of each case is performed and corrections are initiated if needed.
- The process is under supervision of the AA

End of Session

- Thank you very much
- Any question?