Commandes de vol électriques Airbus: une approche globale de la sûreté de fonctionnement
AIRBUS Fly-by-Wire

• Safety process & trade-off
• Fly-by-Wire design for dependability
  ‣ What is « fly-by-wire »
  ‣ dependability threats
    – Physical faults
    – Design & manufacturing errors
    – Particular risks
    – Human-Machine Interface
## SAFETY REQUIREMENT ALLOCATION

### SAFETY SEVERITY CLASSES AND ASSOCIATED OBJECTIVES

<table>
<thead>
<tr>
<th>Class</th>
<th>Objectives at FC level</th>
<th>Objectives at Aircraft level</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATASTROPHIC</td>
<td>$\leq 10^{-9}/hr +$ Fail Safe criterion</td>
<td>$\leq 10^{-7}/hr +$ Fail Safe criterion</td>
</tr>
<tr>
<td>HAZARDOUS</td>
<td>$\leq 10^{-7}/hr$</td>
<td>no objective</td>
</tr>
<tr>
<td>MAJOR</td>
<td>$\leq 10^{-5}/hr$</td>
<td>no objective</td>
</tr>
<tr>
<td>MINOR</td>
<td>no objective</td>
<td>no objective</td>
</tr>
</tbody>
</table>

*Gradation of effort*  
*Assumption of less than 100 Cat. FC*

*Quantitative & qualitative*

FC: Failure Condition
SAFETY PROCESS

TOP (AIRCRAFT) - DOWN (COMPONENT) PROCESS

requirements allocation

SAFETY PROCESS

BOTTOM - UP evaluation

Safety & Reliability method and process
- Research,
- Standards,
- Processes,
- Methods,
- Guidelines,
- Tools,
- In service follow up
- S/R Rules and recom.
- Regulation

Airworthiness regulation, MMEL

A/C Requirements/CRI, Significant Items, Aircraft S/R Reviews

System S/R Reviews, Interface S/R Activities

Multi program, multi disciplinary activities

Multi system activities on one program

System/equipment activities on one program

Common Cause activities on one program

Multi disciplinary activities

Multi program, multi disciplinary activities

Multi system activities on one program

System/equipment activities on one program

Common Cause activities on one program

Multi disciplinary activities

SAFETY PROCESS

TOP (AIRCRAFT) - DOWN (COMPONENT) PROCESS

requirements allocation
SAFETY PROCESS

Top level requirements

Cost requirements

Top Level Program Requirements

Top Level Product Requirements

Previous A/C design and “In service” experience

Airworthiness regulation, MMEL

Aircraft manufacturer directives

11-Airworthiness monitoring

12-Lessons learned

Aircraft in service

1- S/R Common Data Document

2- Aircraft FHA

(Functional Hazard Analysis)

3- System S/R Requirements document

4- System function list and System FHA

5- PSSA: Prelim. system Safety Assessment

6- Equipment S/R Requirements

7- Equipment level Safety/Reliability studies (FMEA/FMES, etc.)

8- COMMON CAUSE ANALYSIS (CCA):

- PRA (Particular Risk Analysis)
- ZSA (Zonal Safety Analysis)
- CMA (Common Mode Analysis)

9a- PSSA first flight

9b- SSA System Safety Assessment and MMEL safety justification

10- Aircraft Safety/Reliability Synthesis

11- Airworthiness monitoring

12- Lessons learned

Safety & Reliability method and process

- Research,
- Standards,
- Processes,
- Methods,
- Guidelines,
- Tools,
- In service follow up
- S/R Rules and recom.
- Regulation

Previous A/C design and “In service” experience

1- S/R Common Data Document

2- Aircraft FHA

(Functional Hazard Analysis)

3- System S/R Requirements document

4- System function list and System FHA

5- PSSA: Prelim. system Safety Assessment

6- Equipment S/R Requirements

7- Equipment level Safety/Reliability studies (FMEA/FMES, etc.)

8- COMMON CAUSE ANALYSIS (CCA):

- PRA (Particular Risk Analysis)
- ZSA (Zonal Safety Analysis)
- CMA (Common Mode Analysis)

9a- PSSA first flight

9b- SSA System Safety Assessment and MMEL safety justification

10- Aircraft Safety/Reliability Synthesis

11- Airworthiness monitoring

12- Lessons learned

Safety & Reliability method and process

- Research,
- Standards,
- Processes,
- Methods,
- Guidelines,
- Tools,
- In service follow up
- S/R Rules and recom.
- Regulation

Previous A/C design and “In service” experience

Top level requirements

Cost requirements

Top Level Program Requirements

Top Level Product Requirements

Previous A/C design and “In service” experience

Top level requirements

Aircraft in service

LESSONS LEARNED

IN-SERVICE AIRCRAFT

A/C Requirements/CRI, Significant Items, Aircraft S/R Reviews

System S/R Reviews , Interface S/R Activities

Multi program, multi disciplinary activities

Multi system activities on one program

System/equipment activities on one program

Common Cause activities on one program

Multi disciplinary activities
SAFETY PROCESS

COMMON CAUSE ANALYSIS:
- Particular Risk Analysis
- Zonal Safety Analysis
- Common Mode Analysis
- Human Hazard Analysis

A/C Requirements/CRI, Significant Items, Aircraft S/R Reviews
System S/R Reviews, Interface S/R Activities

Multi program, multi disciplinary activities
Multi system activities on one program
System/equipment activities on one program
Common Cause activities on one program
Multi disciplinary activities
ARCHITECTURE DESIGN / trade-off (QAWA)

• Quantification of Availability & Weight of an Architecture

› Handling quality and flight control system characterisation for global aircraft optimisation (strong inter-dependency)

› Consolidated Safety (control availability), Weight, Dispatch Reliability, and Power needs evaluation (flight control and hydraulic)

› Common core methods and Matlab modules
ARCHITECTURE DESIGN / trade-off (structural loads)

\[ SF \]

\[ SF \text{ is the achieved Safety Factor} \]
\[ \text{Loads to be considered can be due to a design gust, when a Load Alleviation System is unavailable (} \frac{SF \text{ = Ultimate loads}}{\text{loads due to manoeuvre, gust, ... not alleviated}} \text{) or the sum of loads due to a continuing failure (surface oscillation) and of all design loads} \]
\[ \frac{\lambda}{T} \text{ is the probability per flight hour of the failure} \]
\[ T \text{ is an exposure time during which loads are not alleviated} \]

- Reduced aircraft weight
- Increased system cost
- And/or decreased reliability
AIRBUS Fly-by-Wire

• Safety process & trade-off

• Fly-by-Wire design for dependability
  ‣ What is « fly-by-wire »
  ‣ dependability threats
    – Physical faults
    – Design & manufacturing errors
    – Particular risks
    – Human-Machine Interface
AIRBUS FLY-BY-WIRE: BACKGROUND

SAFETY

AVAILABILITY

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.
What is Fly-by-Wire?

From Mechanical Flight Control System….

to … “Fly-By-Wire”….or Electrical Flight Control System (EFCS) …. or “Commandes de Vol électriques” (CDVE)
What is Fly-by-Wire?

From Fly-by-Wire ….

to … “Fly-by-Wire” associated to “Power-by-Wire”.

HYDRAULIC and ELECTRICAL POWER
AIRBUS Fly-by-Wire

• Safety process & trade-off
• Fly-by-Wire design for dependability
  ‣ What is « fly-by-wire »
  ‣ dependability threats
    – Physical faults
    – Design & manufacturing errors
    – Particular risks
    – Human-Machine Interface
AIRBUS Fly-by-Wire

• Safety process

• Fly-by-Wire design for dependability
  ‣ What is « fly-by-wire »
  ‣ dependability threats
    — Physical faults
    — Design & manufacturing errors
    — Particular risks
    — Human-Machine Interface
PHYSICAL FAULTS

COMMAND & MONITORING COMPUTER

SAFETY
PHYSICAL FAULTS

AVAILABILITY

REDUNDANCY
ACTIVE / STAND-BY

P1/Green ➔ P2/Blue ➔ S1/Green ➔ S2/Blue
DESIGN & MANUFACTURING ERROR

Airbus Fly-by-Wire:
- system is developed to ARP 4754 level A
- Computers to DO178B & DO254 level A (plus internal guidelines)

Two types of dissimilar computers are used
- PRIM ≠ SEC

Fault tolerance
DESIGN & MANUFACTURING ERROR

FUNCTIONAL SPECIFICATION

- interface between aircraft & computer sciences
- automatic code generation

- Classical V&V means, plus
  - virtual iron bird (simulation)
  - some formal proof
DESIGN & MANUFACTURING ERROR

PROOF of PROGRAM

Applied on A380 FbW software,
on a limited basis
credit for certification

Method appraisal on-going on system functional specification
DESIGN & MANUFACTURING ERROR

FAULT TOLERANCE

- SEC simpler than PRIM
- PRIM HW ≠ SEC HW
- 4 different software
- data diversity

- From “random” dissimilarity to managed one
- Comforted by experience
PARTICULAR RISKS

COMMON POINT AVOIDANCE

- Qualification to environment
- Physical separation
- Ultimate back-up
PARTICULAR RISKS

ULTIMATE BACK-UP

- Continued safe flight while crew restore computers
- Expected to be Extremely Improbable
- No credit for certification
- From mechanical (A320) to electrical (A380 & A400M)
ELECTRICAL ACTUATION

• A320 ... A340

Avionics

ELECTRICAL GENERATION

EMER GEN  GEN 1  GEN 2  APU GEN

Flight Controls Actuators

HYDRAULIC GENERATION

GREEN PUMP  YELLOW PUMP  BLUE PUMP

• A380 A400M

Avionics

ELECTRICAL GENERATION

EMER GEN  GEN 1  GEN 2  APU GEN

Flight Controls Actuators

HYDRAULIC GENERATION

GREEN PUMP  YELLOW PUMP

MORE REDUNDANCY
DISSIMILAR (HYDRAULIC / ELECTRICAL)
INCREASED SEGREGATION
HUMAN-MACHINE INTERFACE

AUTOMATISATION
- Ultimate safety net
- Instant flight management off danger
- Routine tasks

DECISION HELP
- Reduction of workload, stress, complexity
- Pilot as a supervisor
HUMAN-MACHINE INTERFACE

- Flight envelope protections
  - TCAS, TAWS …
  - Airbus protections

Let the crew concentrate on trajectory
• Some lessons

  ‣ The aircraft is safe if
  
    ➔ a global approach is taken (stack of redundancy vs. common point)
    ➔ continuity in the process (design .. Certification .. In-service)
    ➔ management is supportive & pro-active

This document and all information contained herein is the sole property of AIRBUS S.A.S. No intellectual property rights are granted by the delivery of this document and the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of AIRBUS S.A.S. This document and its content shall not be used for any purpose other than that for which it is supplied.

The statements made herein do not constitute an offer. They are based on the mentioned assumptions and are expressed in good faith. Where the supporting grounds for these statements are not shown, AIRBUS S.A.S. will be pleased to explain the basis thereof.