

Presented by

Pascal TRAVERSE
And Isabelle Lacaze & Jean Souyris

AIRBUS FLY-BY-WIRE A TOTAL APPROACH TO DEPENDABILITY

Reference: by Pascal TRAVERSE, Isabelle LACAZE and Jean SOUYRIS, IFIP “World Computer Conference”, in Toulouse, August 2004.

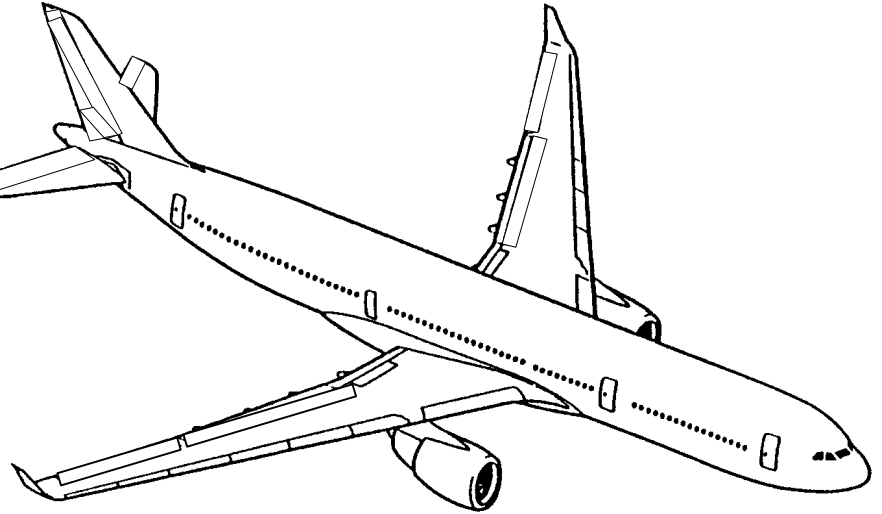
AIRBUS FLY-BY-WIRE A TOTAL APPROACH TO DEPENDABILITY

- Background
 - ▶ What is « fly-by-wire »
 - ▶ Dependability attributes
- Coverage of (some) dependability threats
 - ▶ Physical faults
 - ▶ Design & manufacturing errors
 - ▶ Particular risks
 - ▶ Human-Machine Interface
- Concluding words

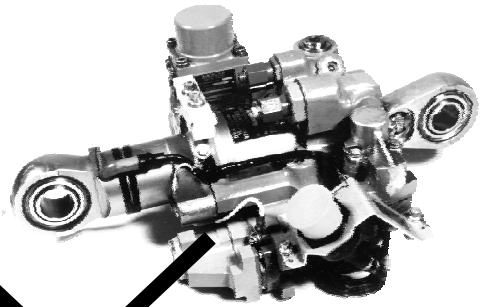
AIRBUS FLY-BY-WIRE: BACKGROUND



SAFETY

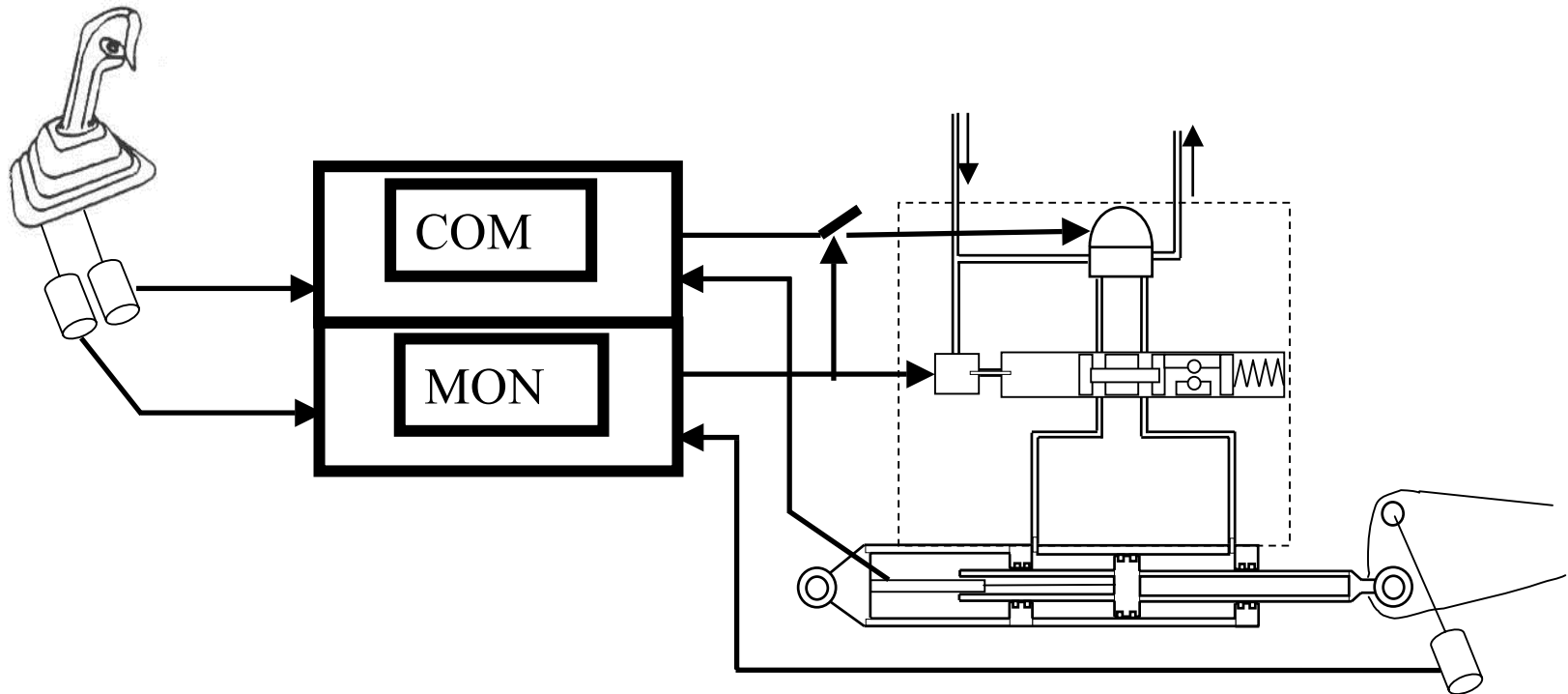


AVAILABILITY



PHYSICAL FAULTS

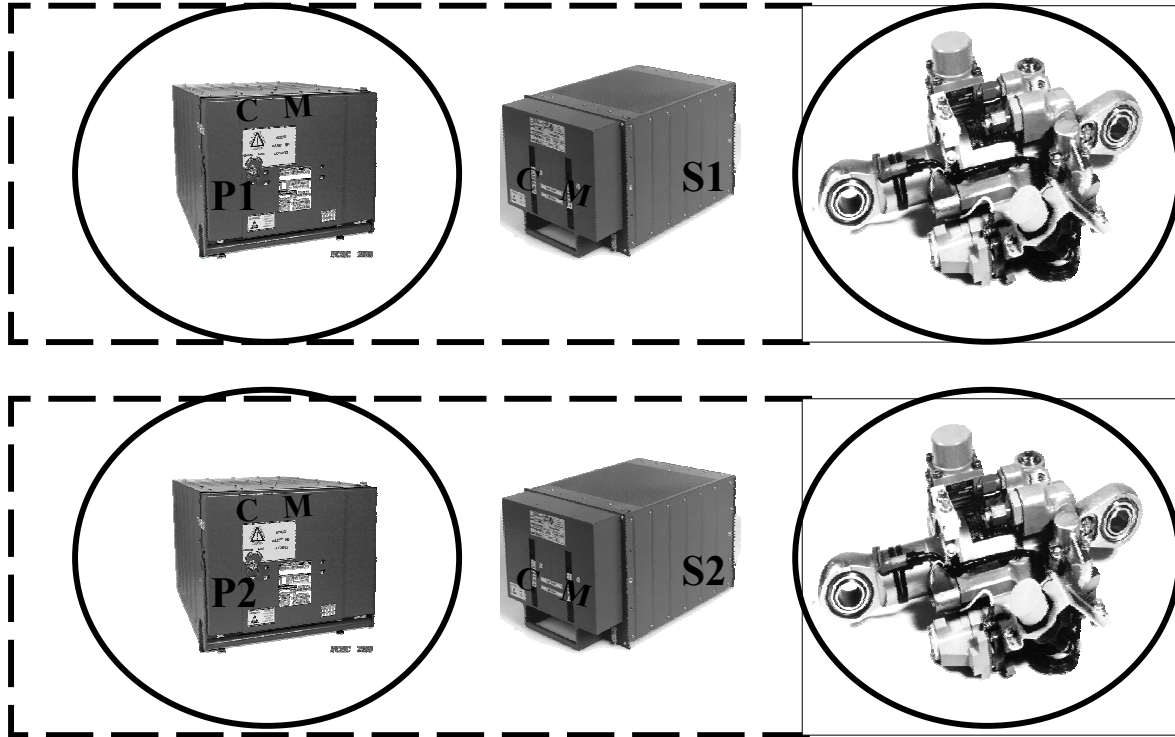
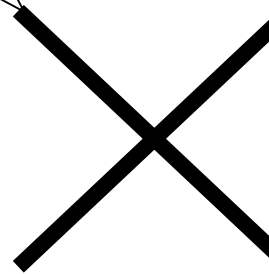
SAFETY



COMMAND & MONITORING COMPUTER

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)

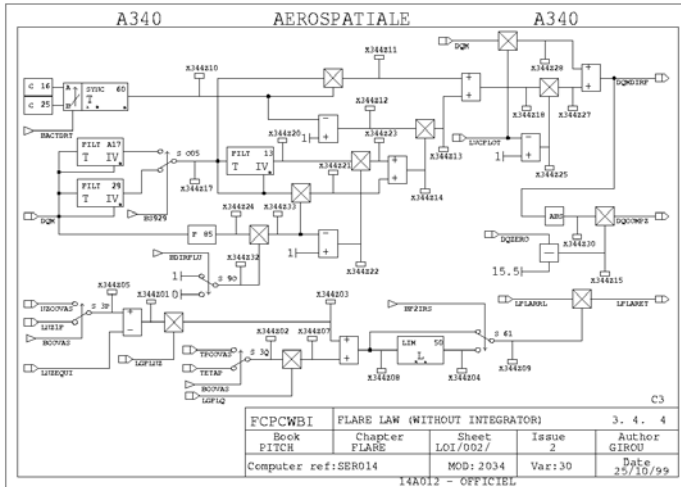
Fault
avoidance

Two types of dissimilar computers are used
PRIM \neq 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

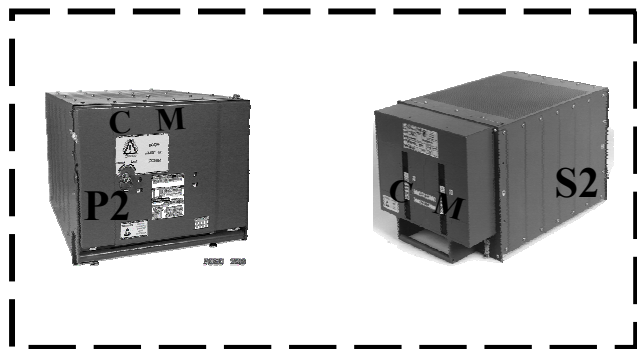
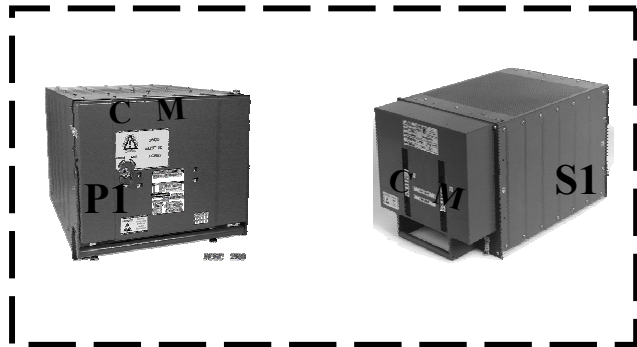
DESIGN & MANUFACTURING ERROR

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

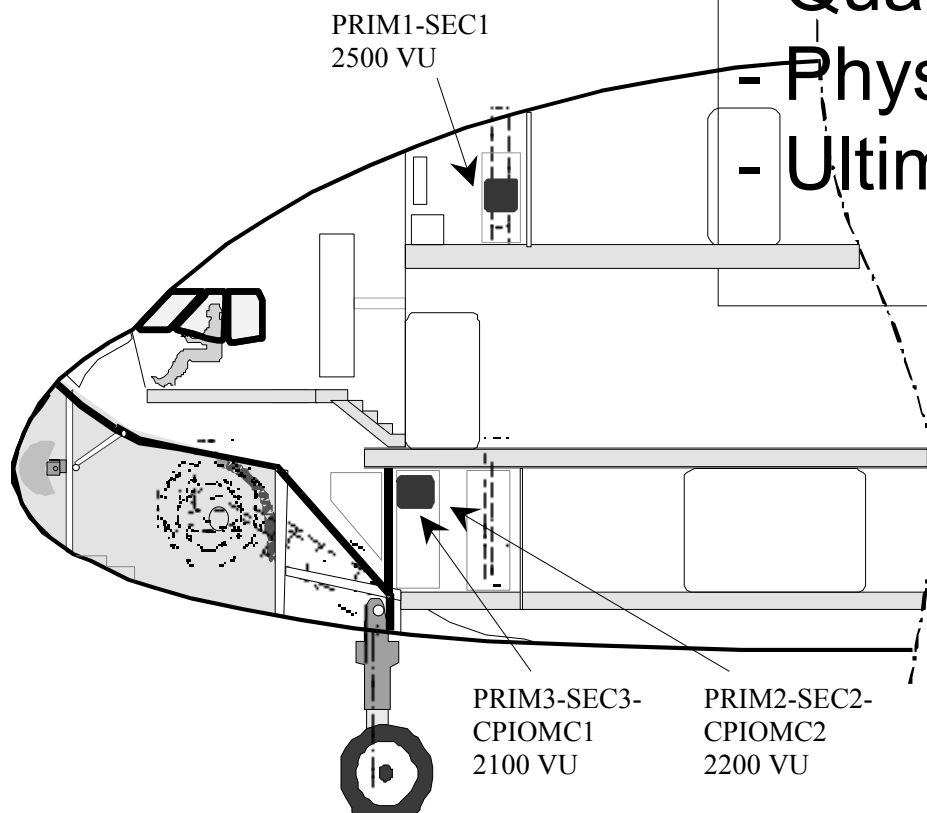
- SEC simpler than PRIM
- PRIM HW \neq SEC HW
- 4 different software
- data diversity

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

PARTICULAR RISKS

COMMON POINT AVOIDANCE

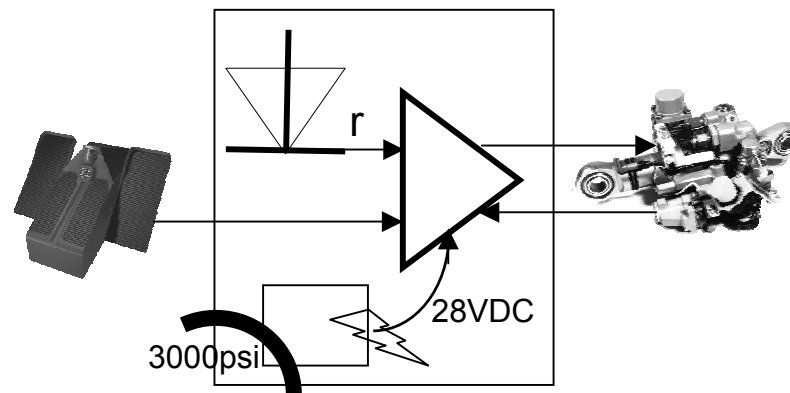
- Qualification to environment
- Physical separation
- Ultimate back-up



PARTICULAR RISKS

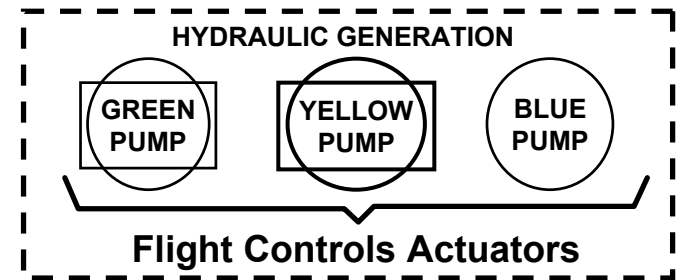
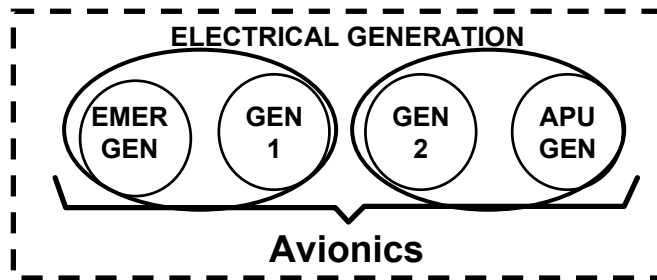
ULTIMATE BACK-UP

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

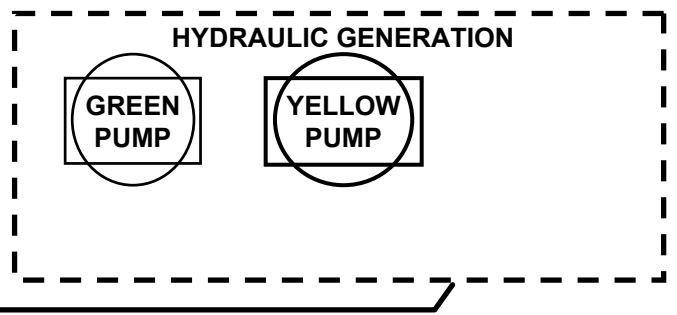
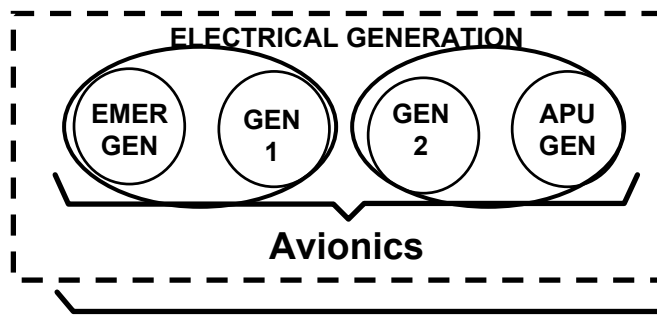


ELECTRICAL ACTUATION

- **A320 ... A340**



- **A380 A400M**



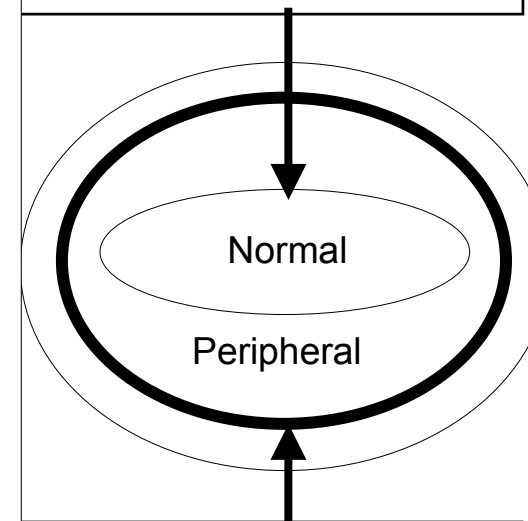
Flight Controls Actuators

**MORE REDUNDANCY
DISSIMILAR (HYDRAULIC / ELECTRICAL)
INCREASED SEGREGATION**

HUMAN-MACHINE INTERFACE

- Reduction of crew workload & fatigue
- Situation awareness
- System reconfiguration
- Flight envelope protections
 - TCAS, TAWS ...
 - Airbus protections

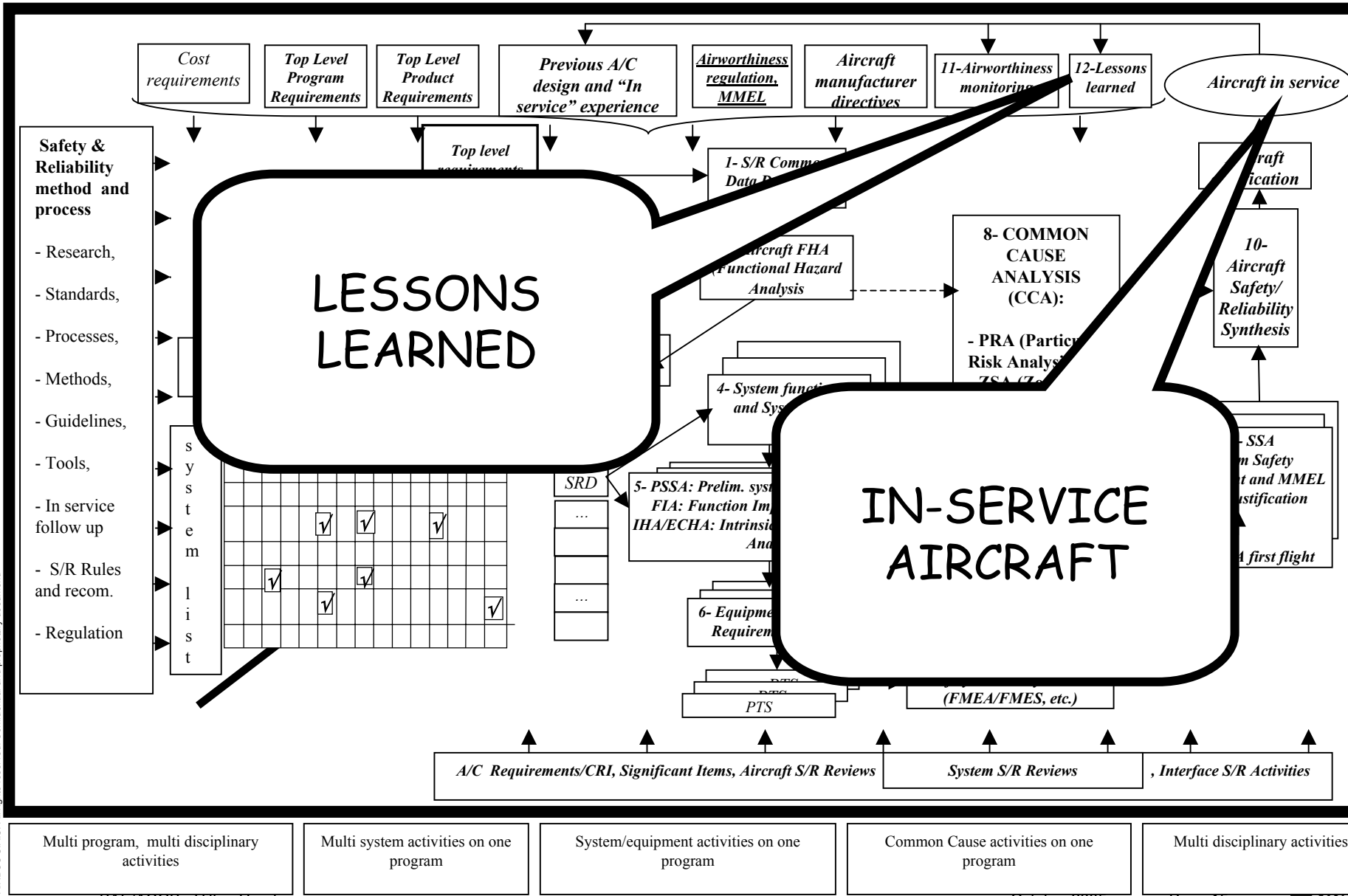
Stick released :
Aircraft will fly inside normal
Flight Envelope



Stick on the stops :
Aircraft will fly
at the maximum safe limit

Let the crew concentrate on trajectory

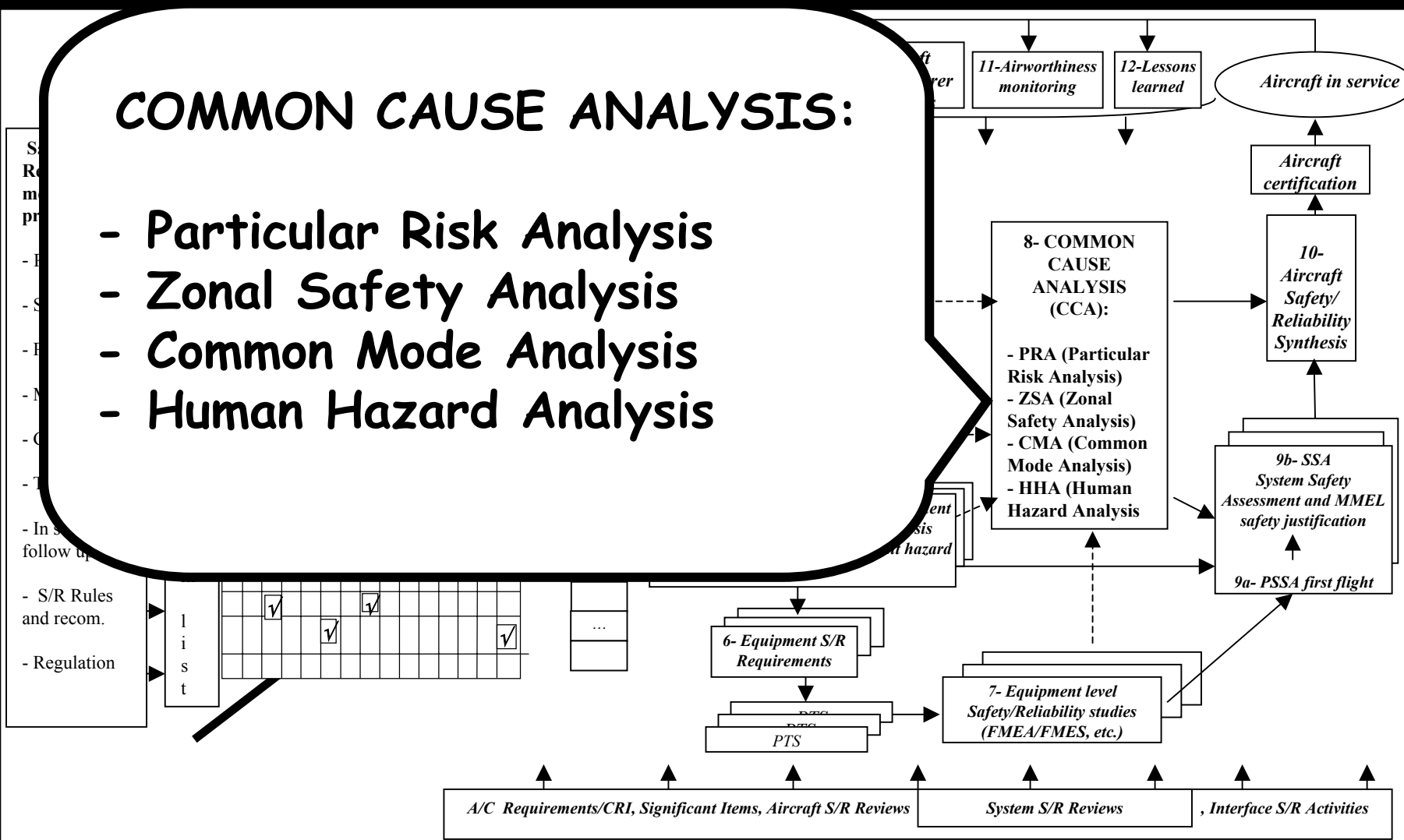
DEPENDABILITY PROCESS



DEPENDABILITY PROCESS

COMMON CAUSE ANALYSIS:

- Particular Risk Analysis
- Zonal Safety Analysis
- Common Mode Analysis
- Human Hazard Analysis



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

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
----------------------------------------------	----------------------------------------	--------------------------------------------	----------------------------------------	-------------------------------

AIRBUS FLY-BY-WIRE A TOTAL APPROACH TO DEPENDABILITY

CONCLUDING WORDS

Joint effort for improvement

- FAA/JAA/... Airbus/Boeing/...
- Regulations and practices improvement based on
 - Type certifications experience
 - In-service incidents & accidents
- For in-service airplane & under design

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.



AIRBUS

**AN EADS JOINT COMPANY
WITH BAE SYSTEMS**