Presented by

Pascal TRAVERSE
And Isabelle Lacaze & Jean Souyris

AIRBUS FLY-BY-WIRE
A TOTAL APPROACH TO DEPENDABILITY

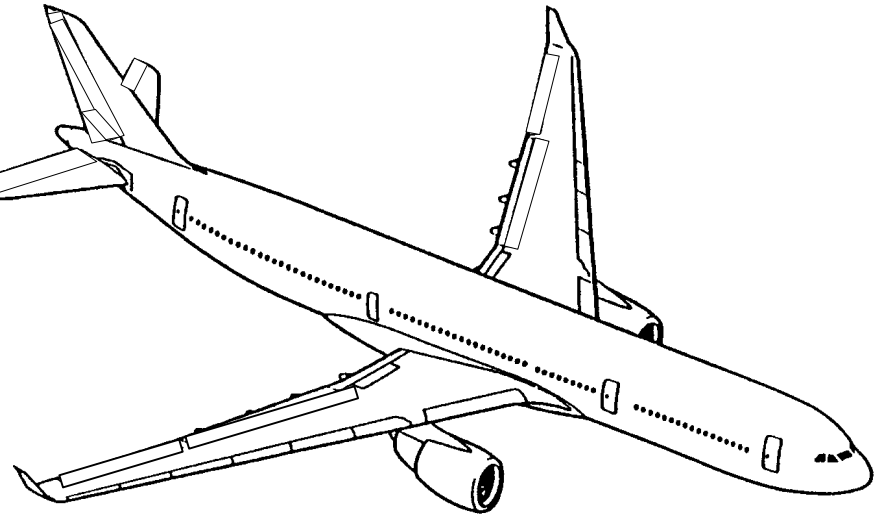
Reference: by Pascal TRAVERSE, Isabelle LACAZE and Jean SOUYRIS, IFIP “World Computer Conference”, in Toulouse, August 2004.

AIRBUS FLY-BY-WIRE
A TOTAL APPROACH TO DEPENDABILITY

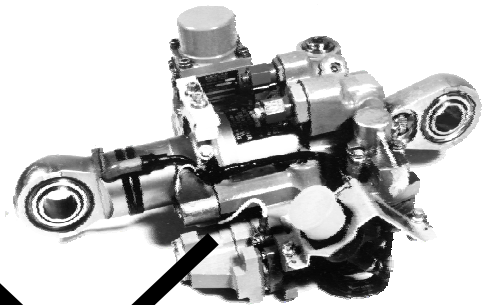
- Background
  - What is « fly-by-wire »
  - Dependability attributes
- Coverage of (some) dependability threats
  - Physical faults
  - Design & manufacturing errors
  - Particular risks
  - Human-Machine Interface
- Concluding words

AIRBUS FLY-BY-WIRE: BACKGROUND

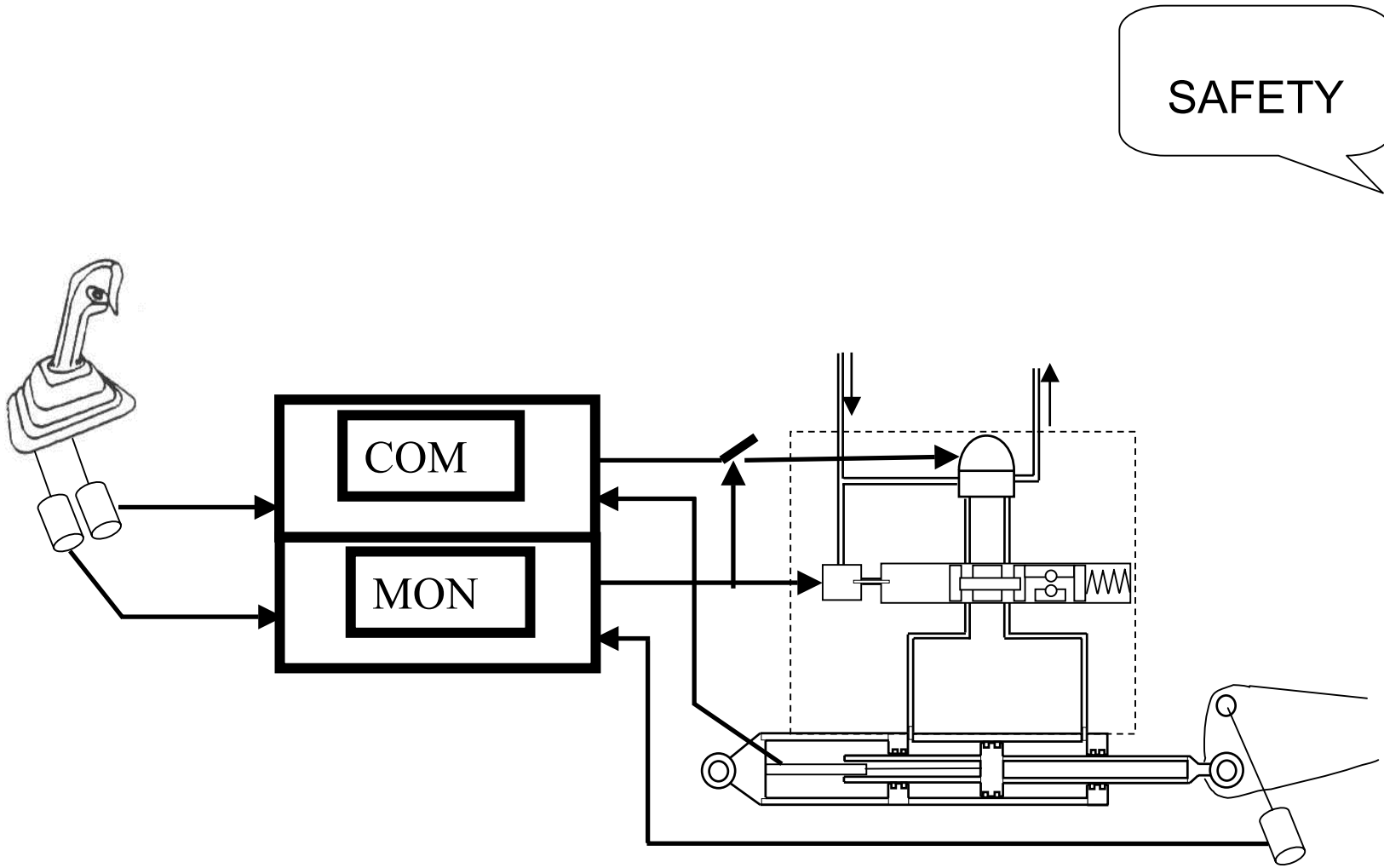
SAFETY



AVAILABILITY



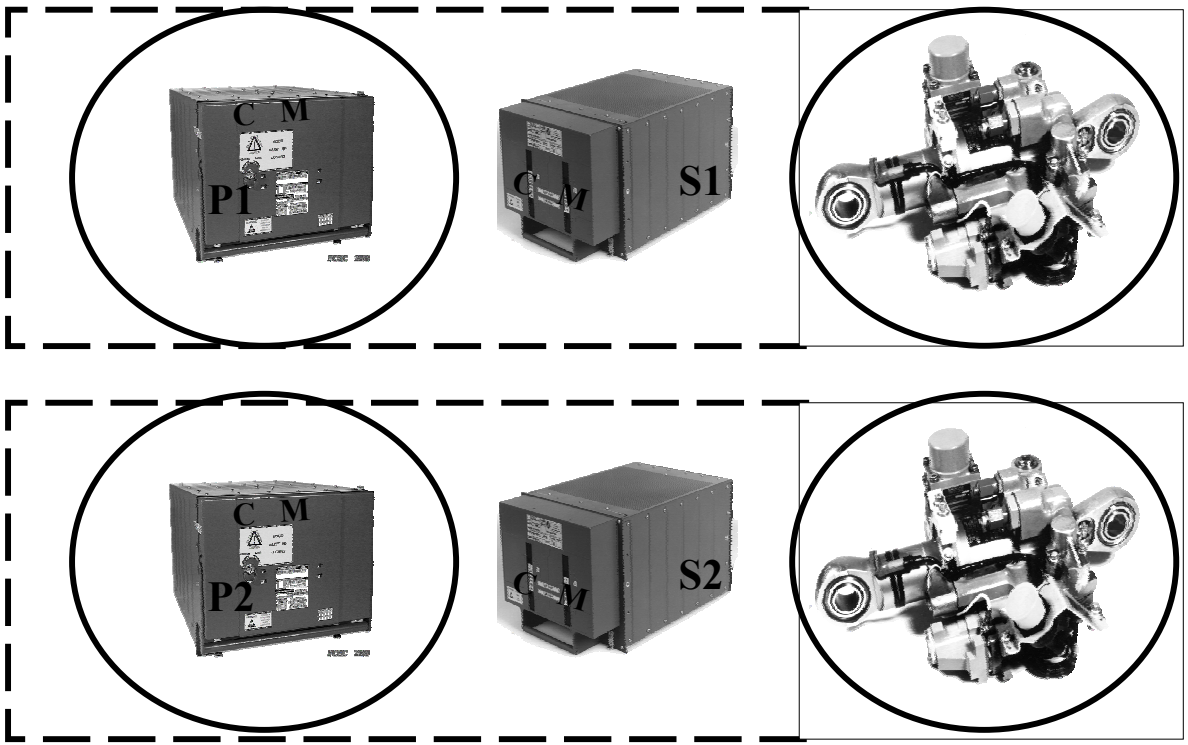
PHYSICAL FAULTS



COMMAND & MONITORING COMPUTER

PHYSICAL FAULTS

AVAILABILITY



REDUNDANCY
ACTIVE / STAND-BY
P1/Green ➔ P2/Blue ➔ S1/Green ➔ S2/Blue

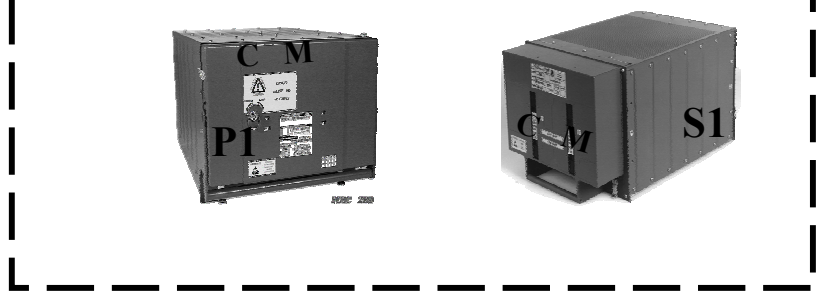
DESIGN & MANUFACTURING ERROR

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

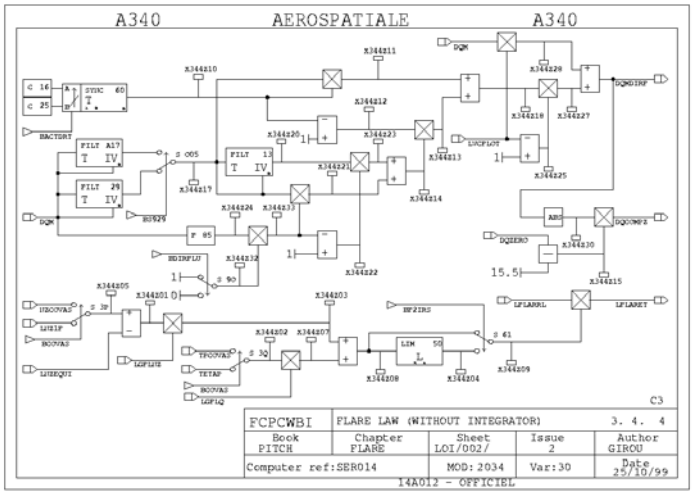
Fault avoidance

Two types of dissimilar computers are used
PRIM ≠ 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

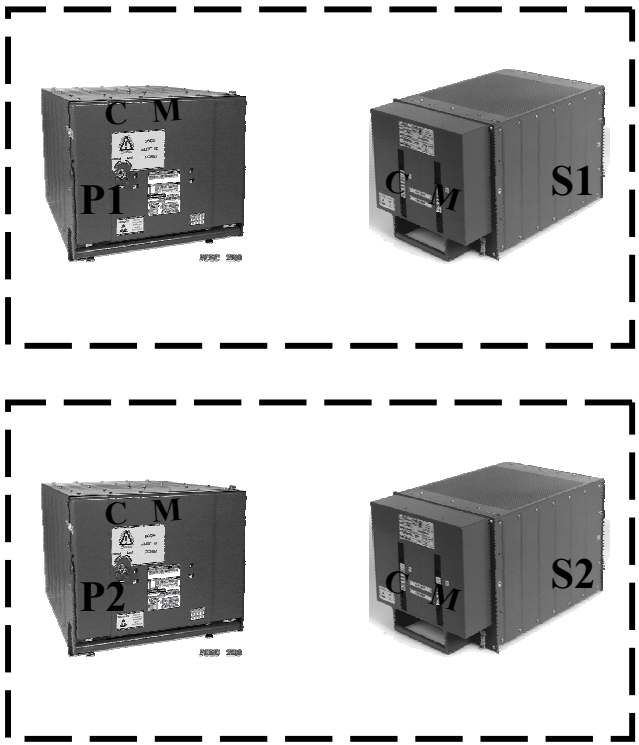
DESIGN & MANUFACTURING ERROR

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

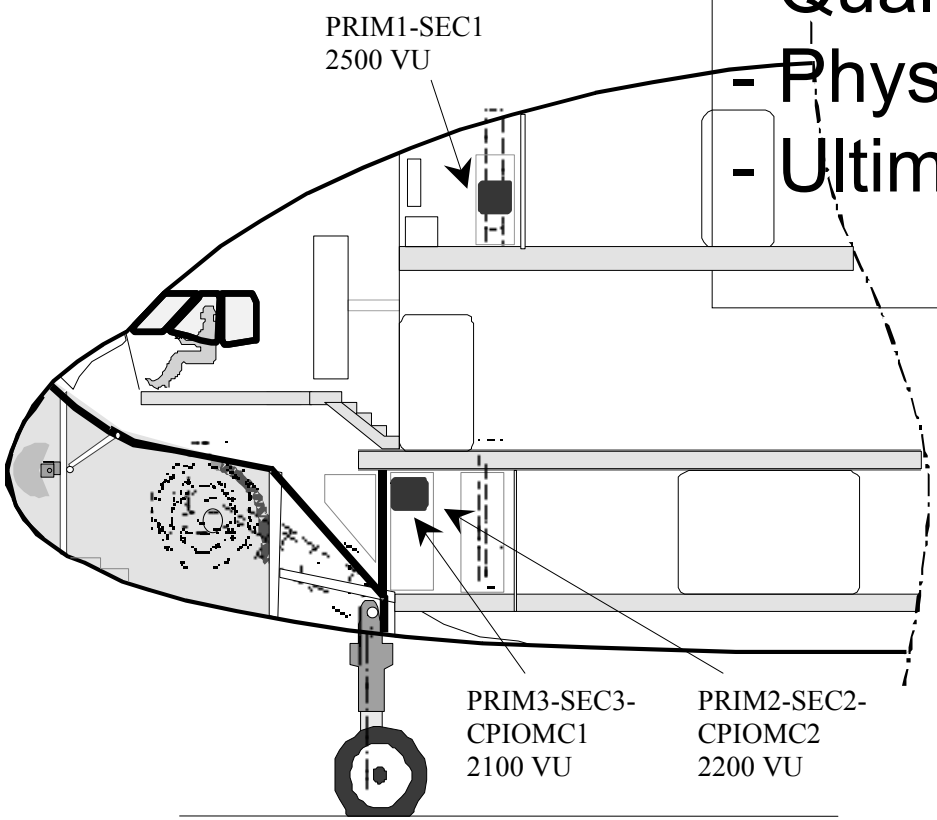
- SEC simpler than PRIM
- PRIM HW ≠ SEC HW
- 4 different software
- data diversity

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

PARTICULAR RISKS

COMMON POINT AVOIDANCE

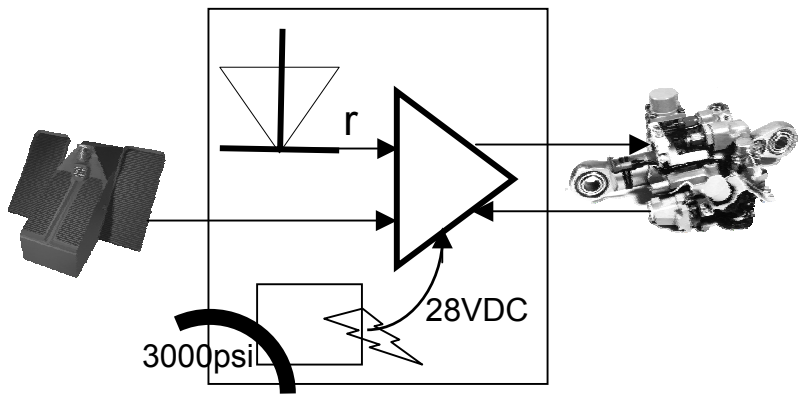
- Qualification to environment
- Physical separation
- Ultimate back-up



PARTICULAR RISKS

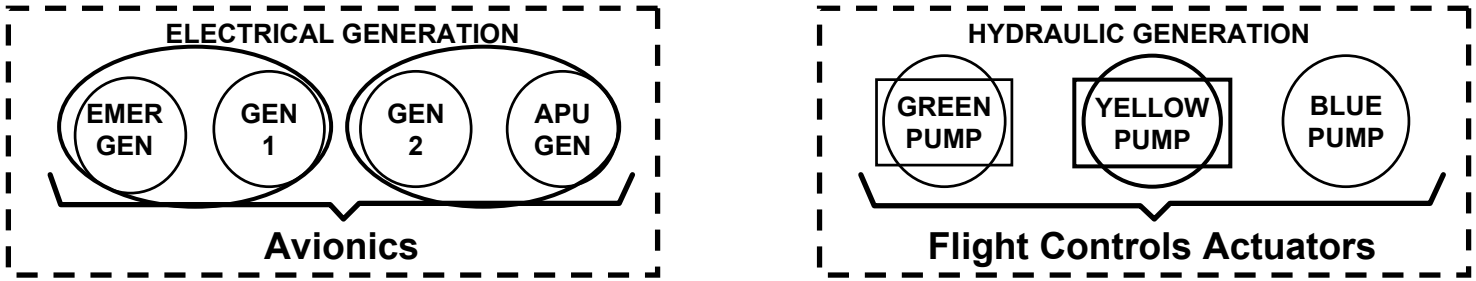
ULTIMATE BACK-UP

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

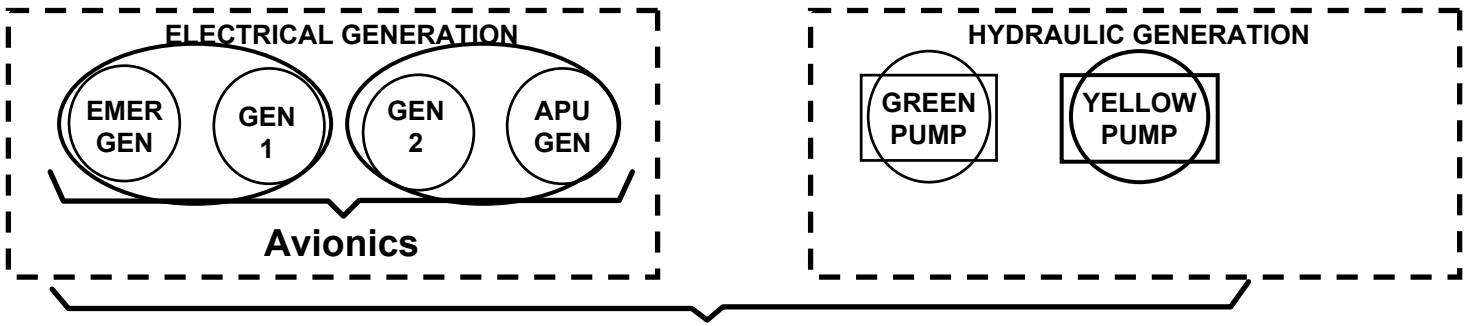


ELECTRICAL ACTUATION

- **A320 ... A340**



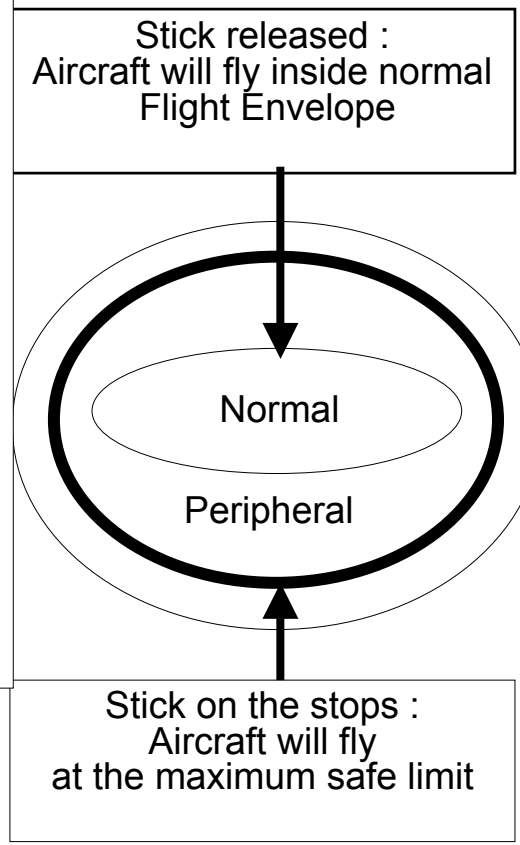
- **A380 A400M**



MORE REDUNDANCY
DISSIMILAR (HYDRAULIC / ELECTRICAL)
INCREASED SEGREGATION

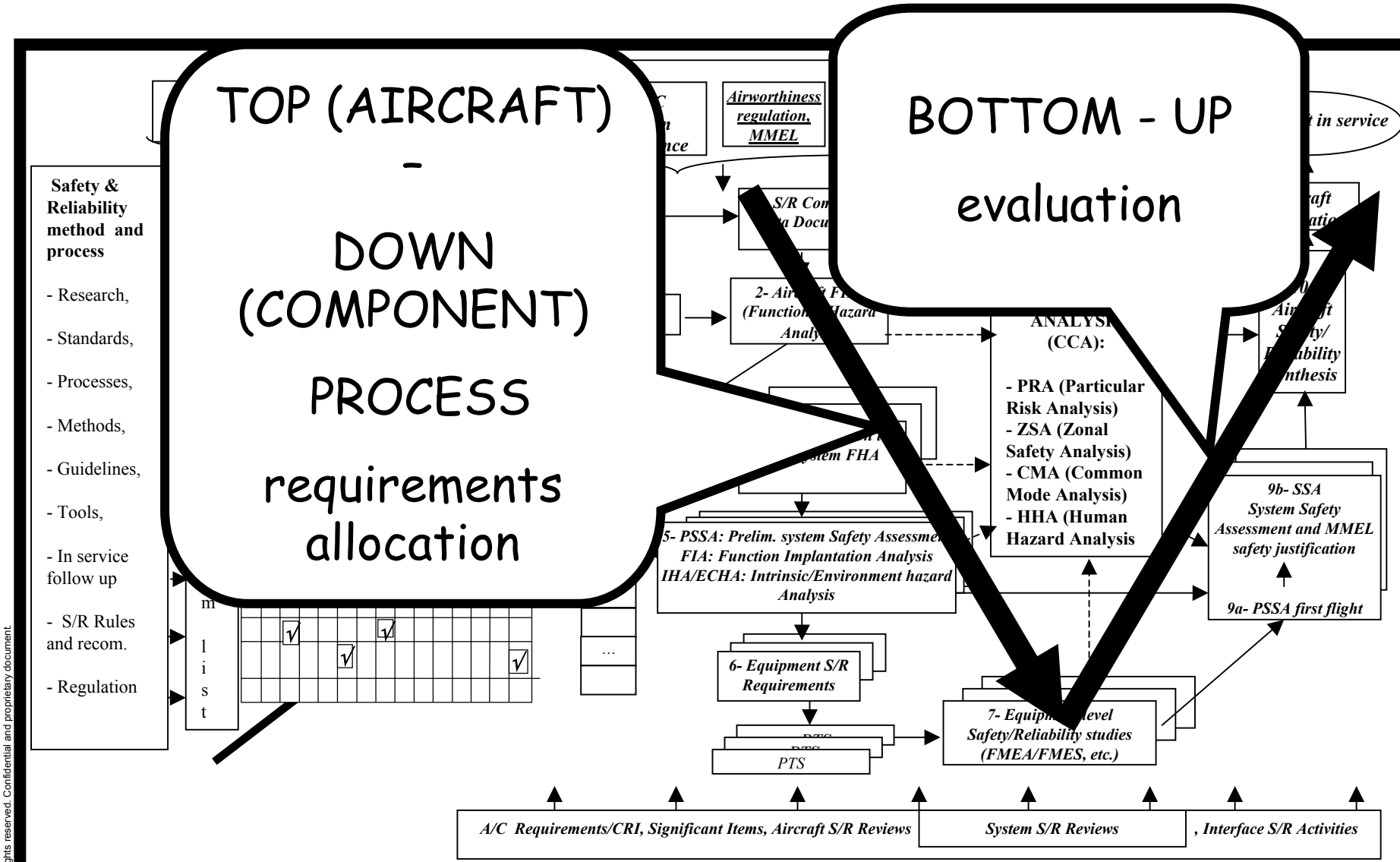
HUMAN-MACHINE INTERFACE

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



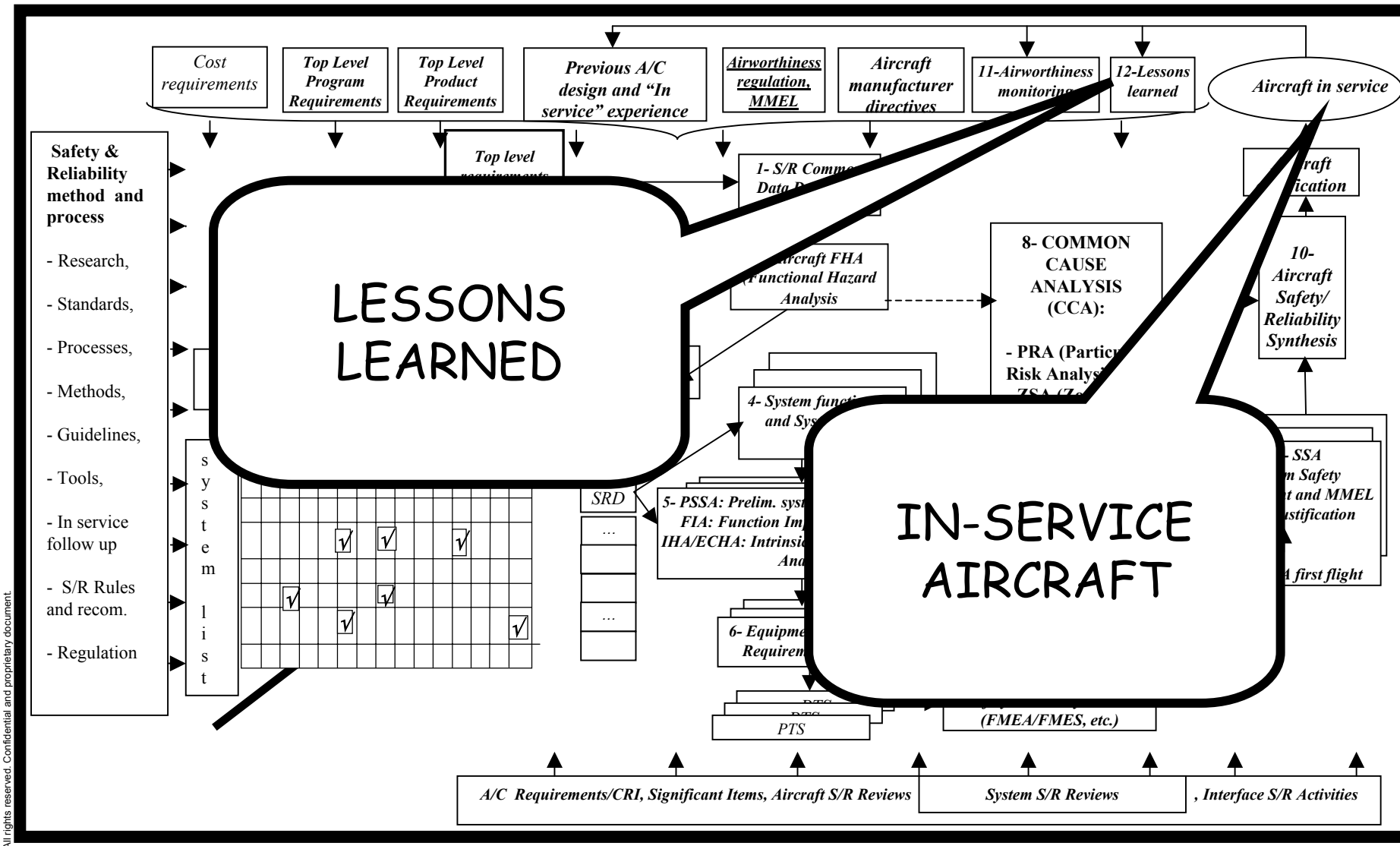
Let the crew concentrate on trajectory

DEPENDABILITY PROCESS



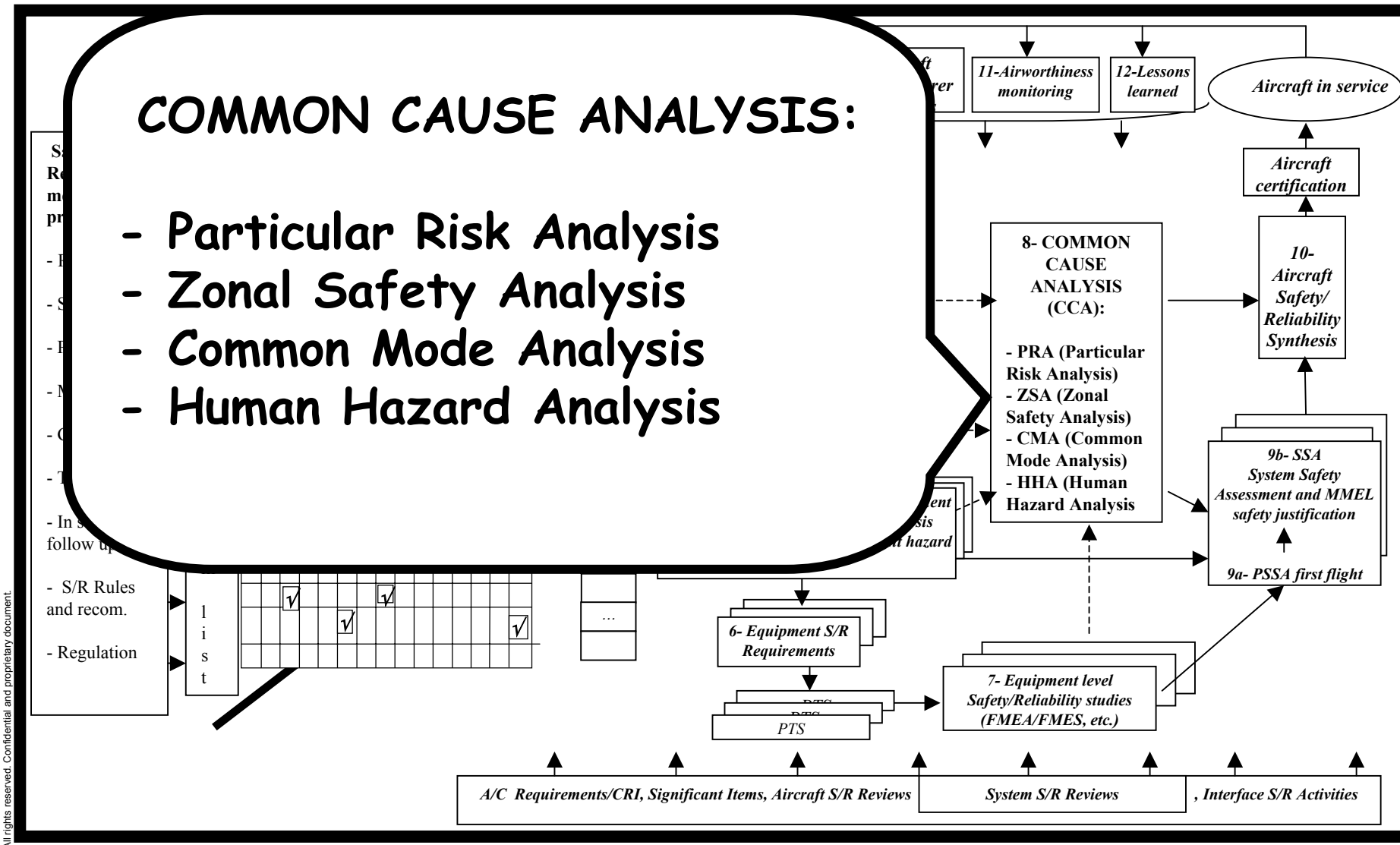
Multi program, multi disciplinary activities	Multi system activities on one program	System/equipment activities on one program	Common Cause activities on one program	Multi disciplinary activities

DEPENDABILITY PROCESS



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

DEPENDABILITY PROCESS



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

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