

Presented by Pascal TRAVERSE

Prepared with Isabelle LACAZE & Jean SOUYRIS

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
- Potential trends for Fly-by-Wire

SAFETY REQUIREMENT ALLOCATION

SAFETY SEVERITY CLASSES AND ASSOCIATED OBJECTIVES

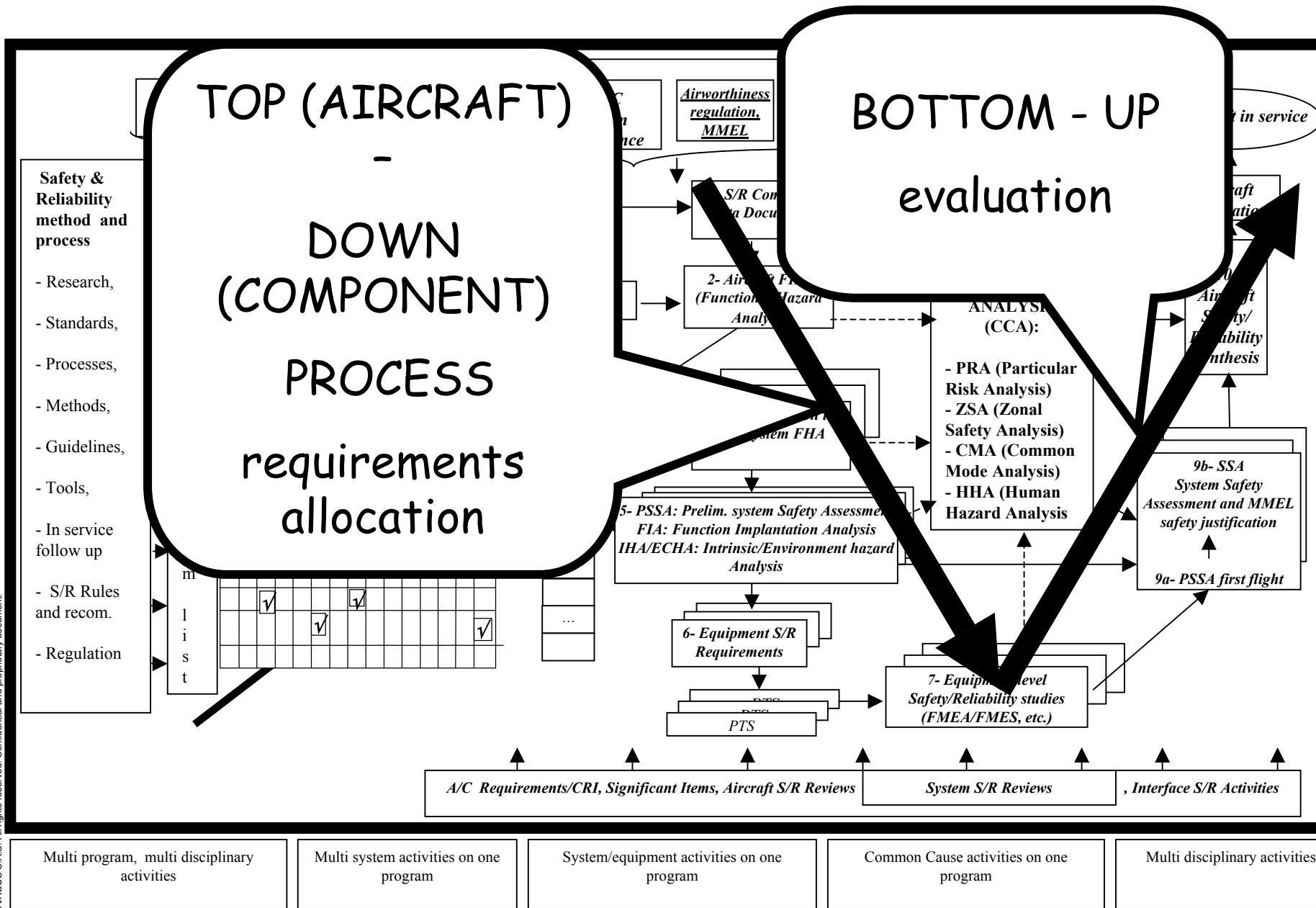
Class	Objectives at FC level	Objectives at Aircraft level
Assumption of less than 100 Cat. EC CATASTROPHIC	$\leq 10^{-9}/\text{hr} +$ Fail Safe criterion	$\leq 10^{-7}/\text{hr} +$ Fail Safe criterion
HAZARDOUS	$\leq 10^{-7}/\text{hr}$	no objective
MAJOR	$\leq 10^{-5}/\text{hr}$	no objective
MINOR	no objective	no objective

Assumption of less than 100 Cat. EC

Quantitative & qualitative

Gradation of effort

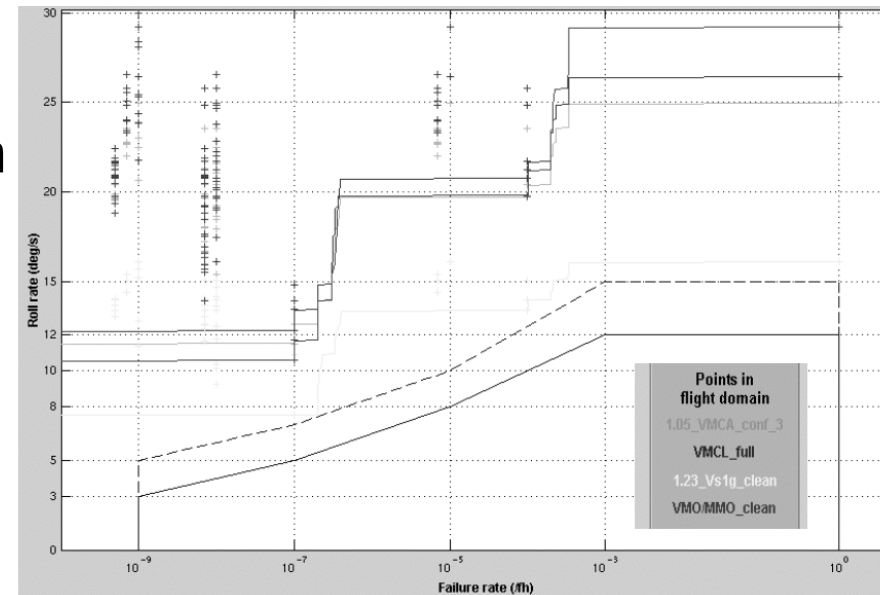
SAFETY PROCESS



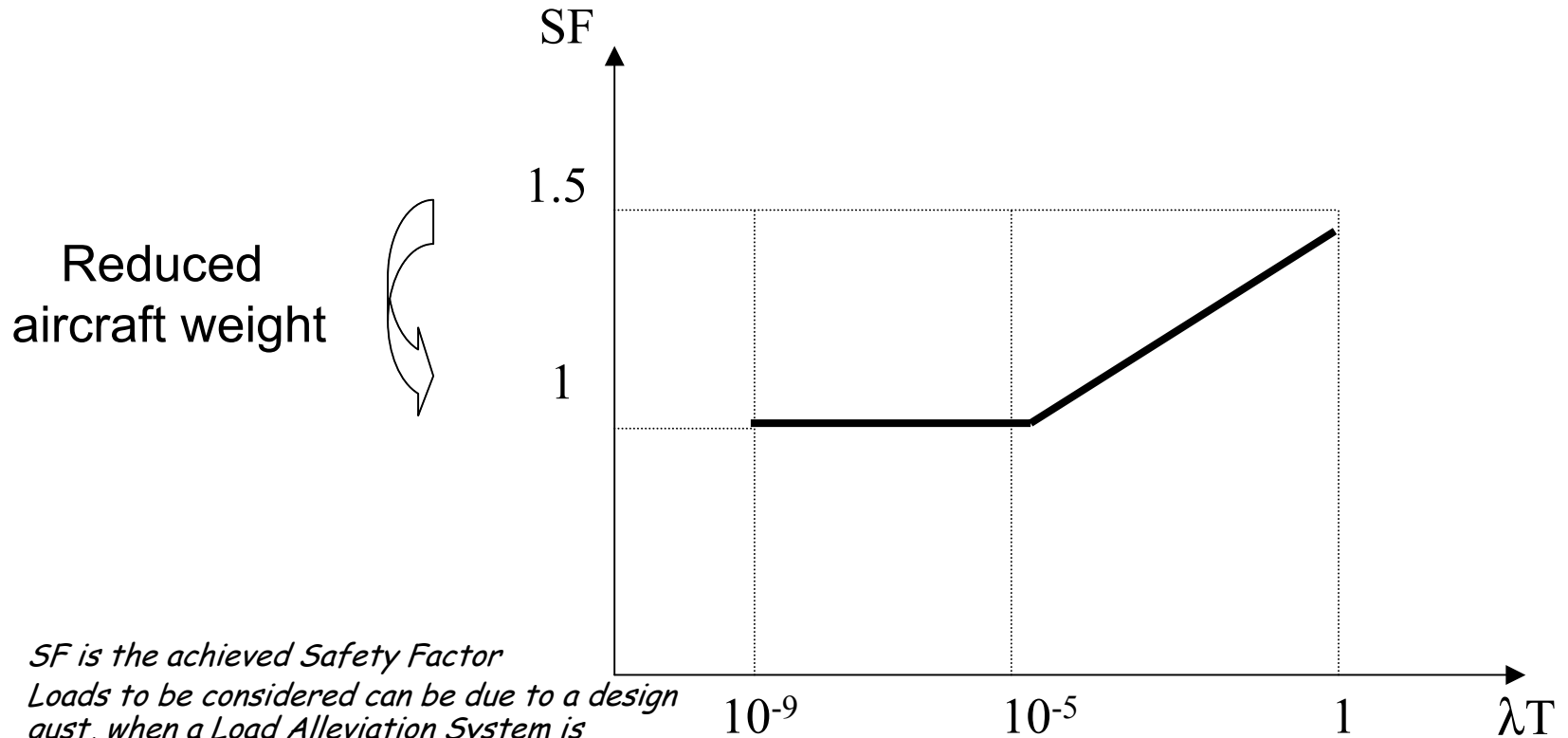
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

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 is the achieved Safety Factor*

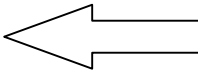
Loads to be considered can be due to a design gust, when a Load Alleviation System is unavailable (SF = Ultimate loads / loads due to manoeuvre, gust, ... not alleviated) or the sum of loads due to a continuing failure (surface oscillation) and of all design loads

λ is the probability per flight hour of the failure

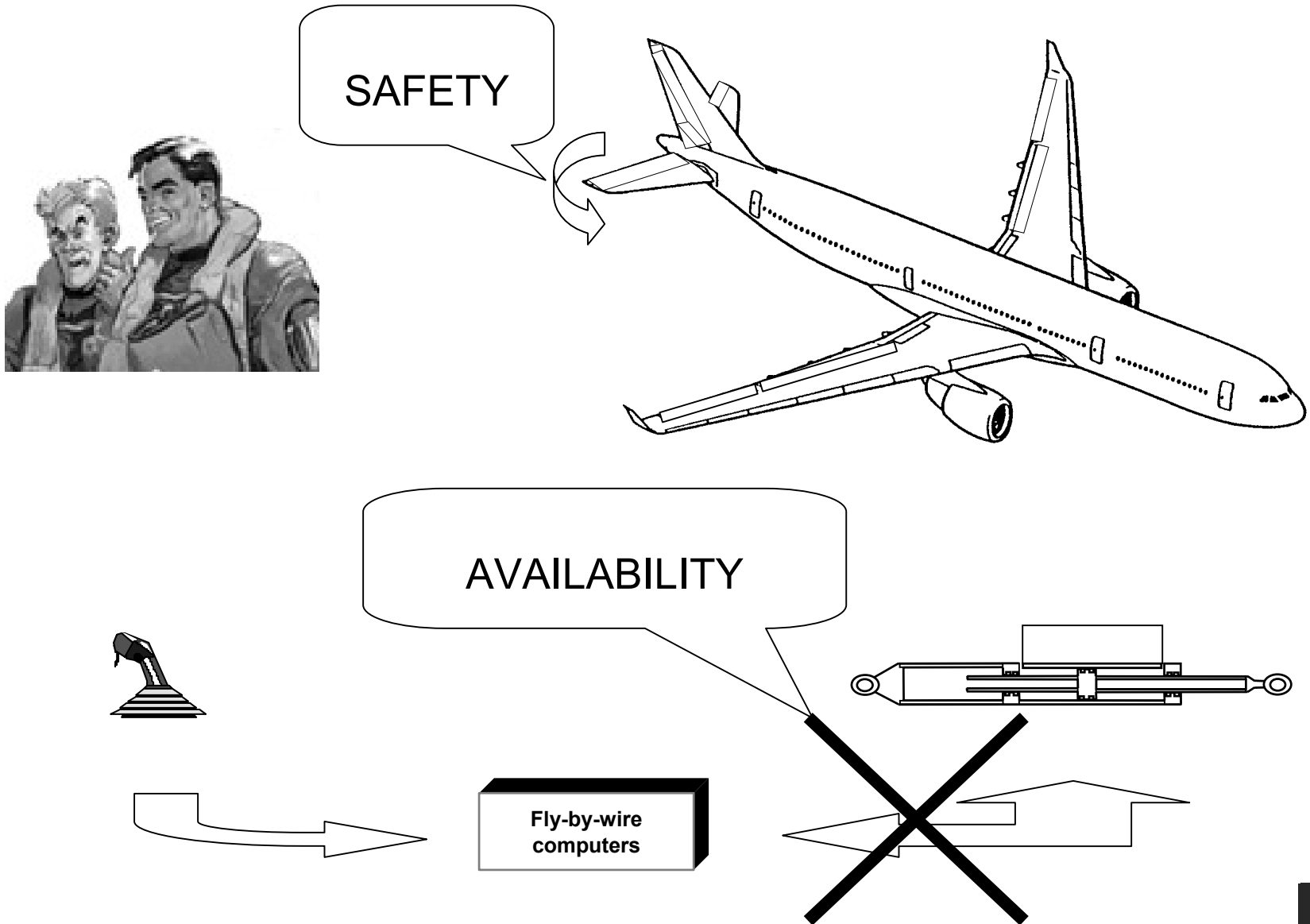
T is an exposure time during which loads are not alleviated

Increased system cost
And/or decreased reliability

AIRBUS Fly-by-Wire

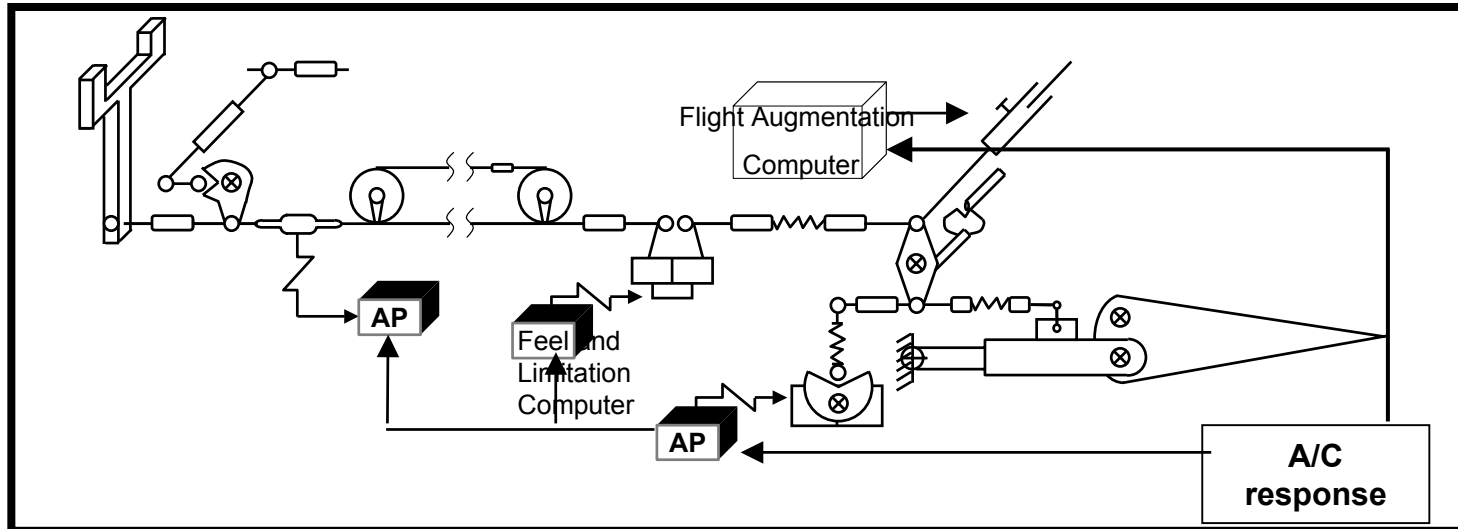
- Safety process & trade-off
- Fly-by-Wire design for dependability
 - ▶ What is « fly-by-wire » 
 - ▶ dependability threats
 - Physical faults
 - Design & manufacturing errors
 - Particular risks
 - Human-Machine Interface
- Potential trends for Fly-by-Wire

AIRBUS FLY-BY-WIRE: BACKGROUND

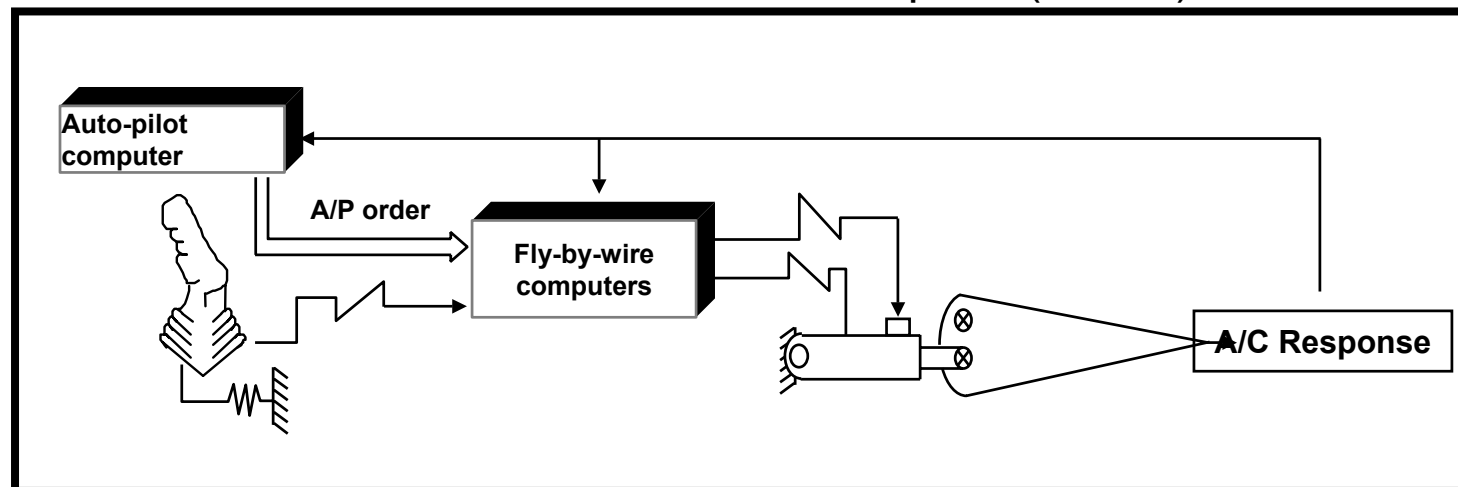


What is Fly-by-Wire?

From Mechanical Flight Control System....

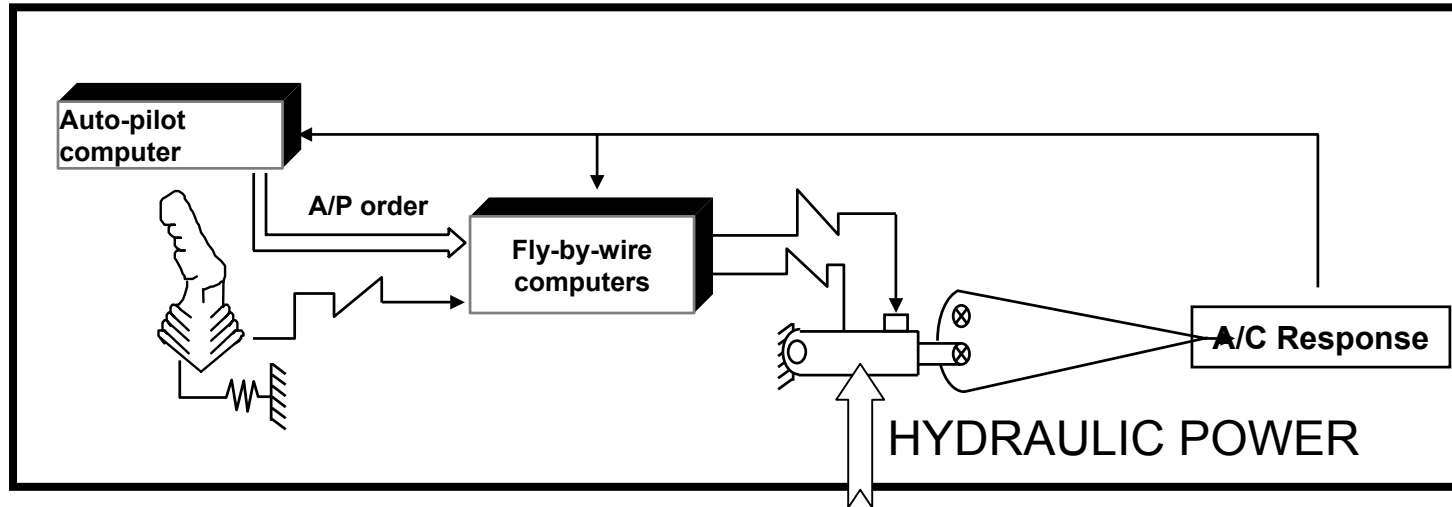


to ... “Fly-By-Wire”....or Electrical Flight Control System (EFCS)
or “Commandes de Vol électriques” (CDVE)

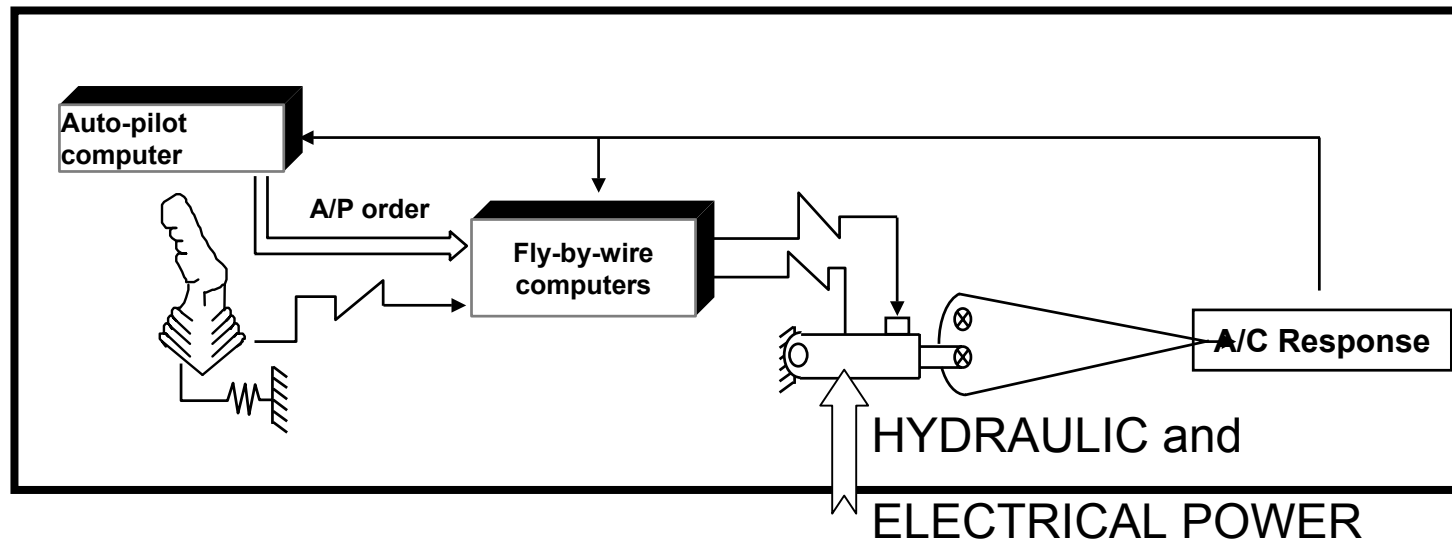


What is Fly-by-Wire?

From Fly-by-Wire



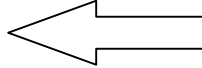
to ... "Fly-by-Wire" associated to "Power-by-Wire".



AIRBUS Fly-by-Wire

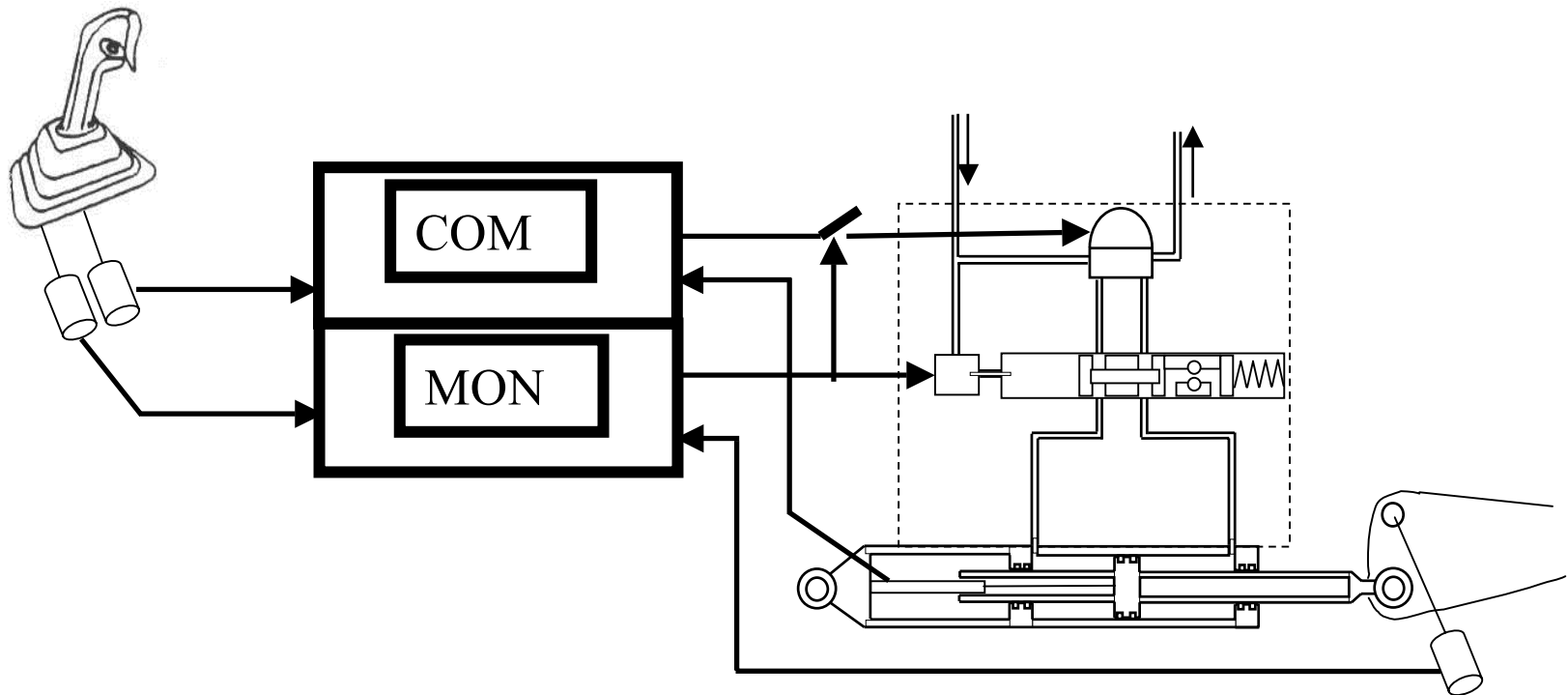
- Safety process & trade-off
- Fly-by-Wire design for dependability
 - ▶ What is « fly-by-wire »
 - ▶ dependability threats
 - Physical faults
 - Design & manufacturing errors
 - Particular risks
 - Human-Machine Interface
- Potential trends for Fly-by-Wire

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
- Potential trends for Fly-by-Wire

PHYSICAL FAULTS

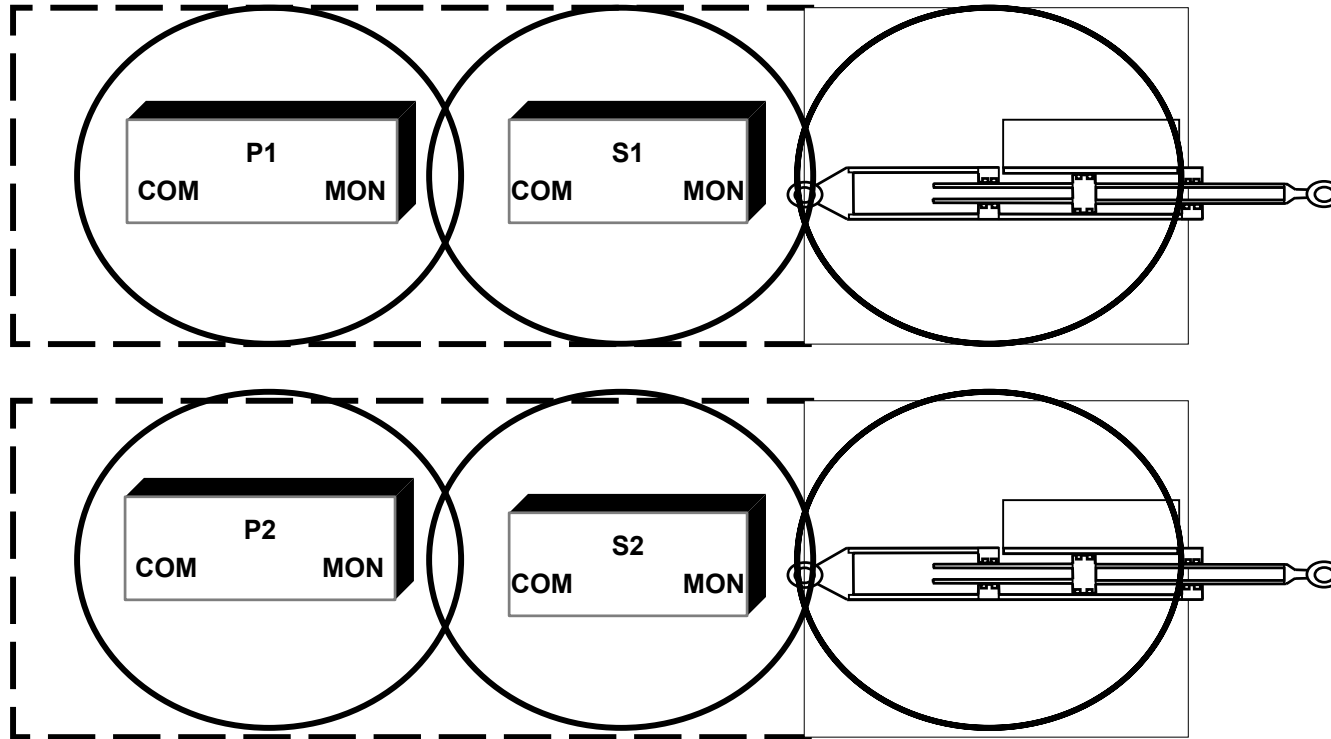
SAFETY



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)

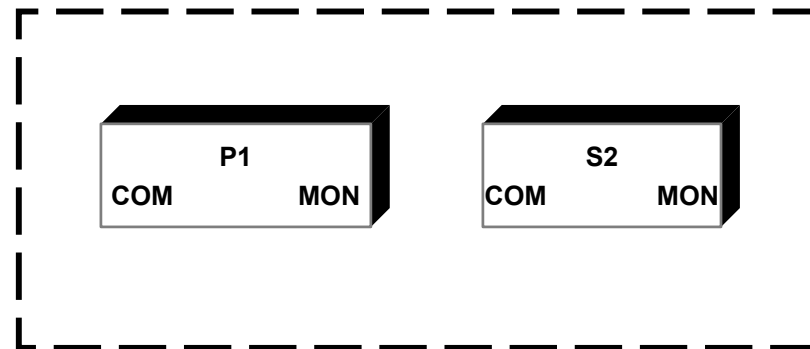


Fault
prevention
& removal

Two types of dissimilar computers are used
PRIM \neq SEC



Fault
tolerance



PROOF of PROGRAM

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

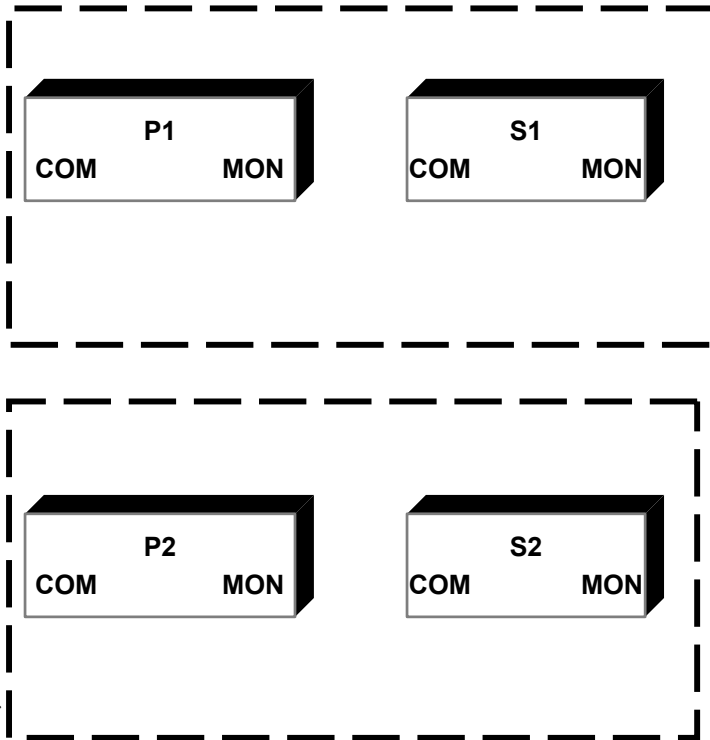
Method appraisal on-going on system functional
specification

DESIGN & MANUFACTURING ERROR

FAULT TOLERANCE

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

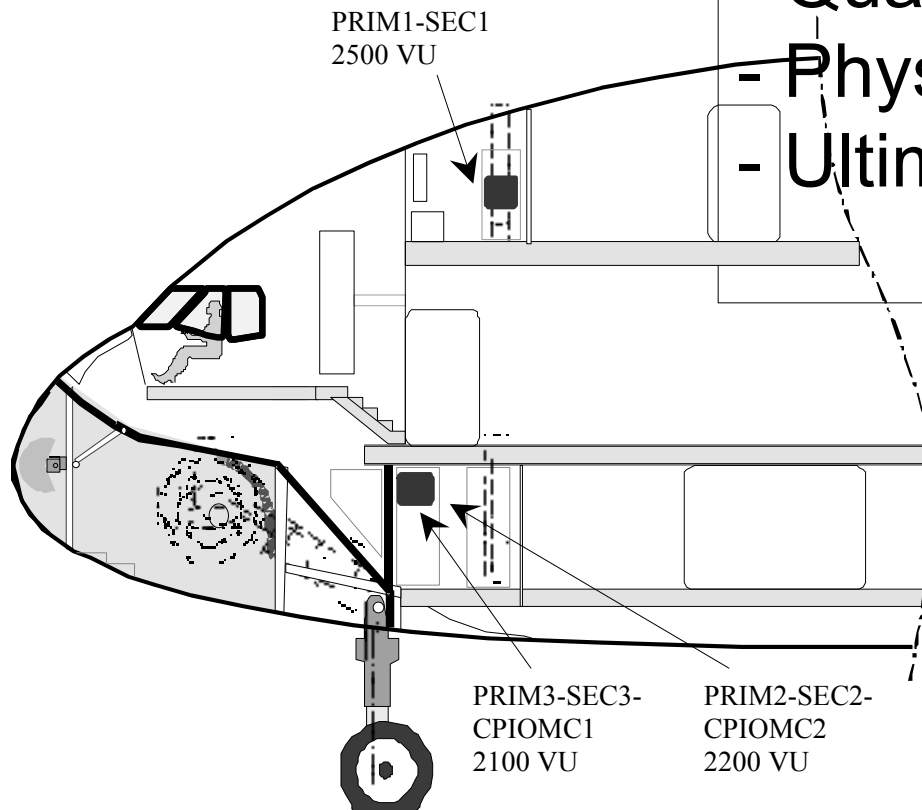
- From “random” dissimilarity to managed one
- Comforted by experience



PARTICULAR RISKS

COMMON POINT AVOIDANCE

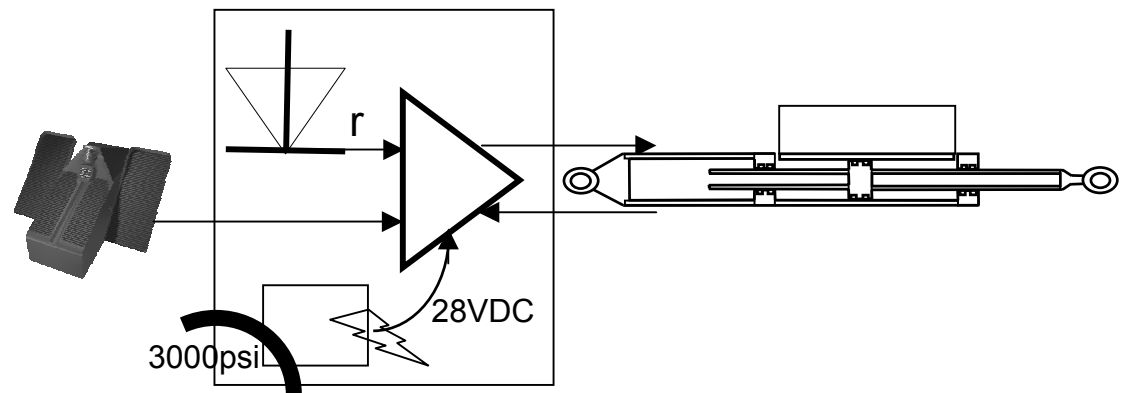
- Qualification to environment
- Physical separation
- Ultimate back-up



PARTICULAR RISKS

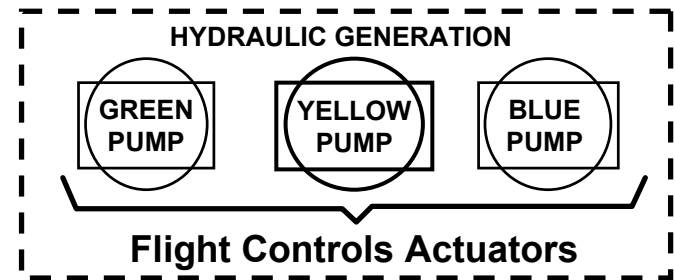
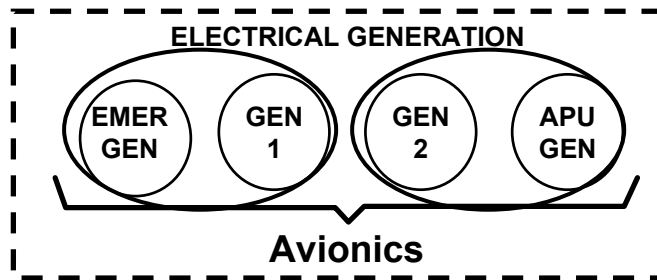
ULTIMATE BACK-UP

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

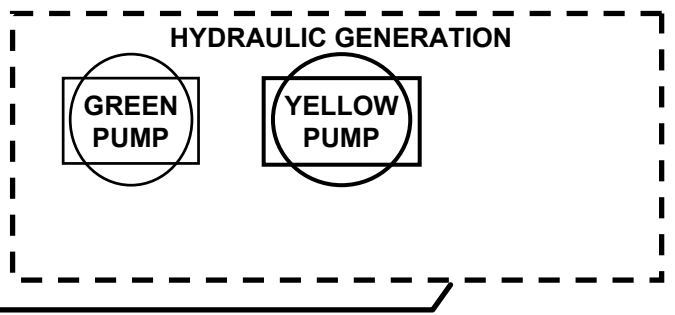
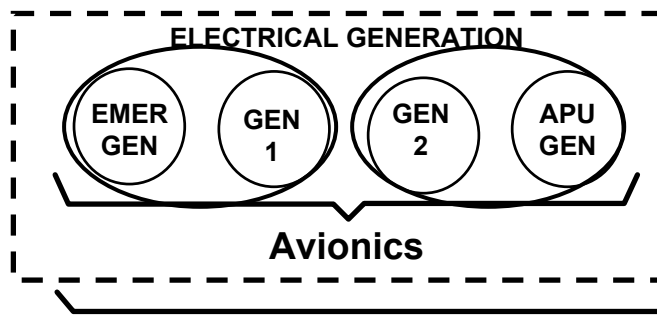


ELECTRICAL ACTUATION

- **A320 ... A340**



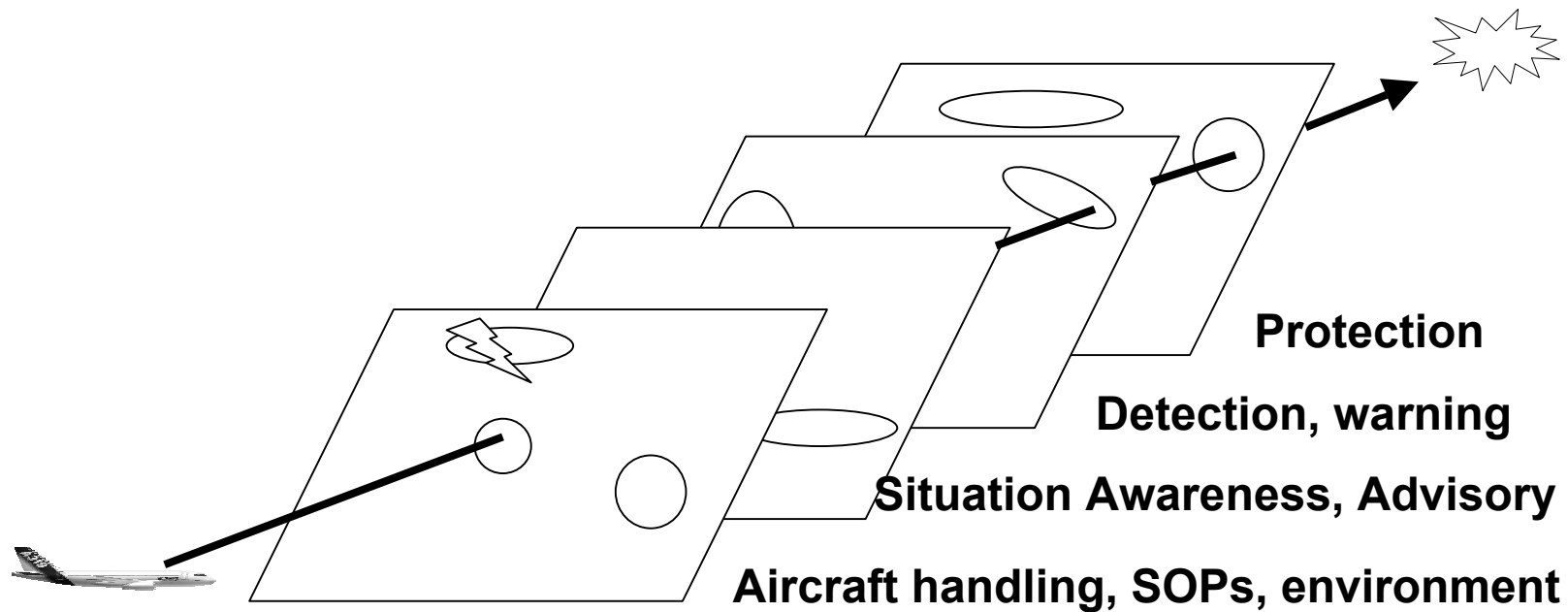
- **A380 A400M**



Flight Controls Actuators

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

HUMAN-MACHINE INTERFACE



AUTOMATISATION

- Ultimate safety net
- Instant flight management of danger
- Routine tasks

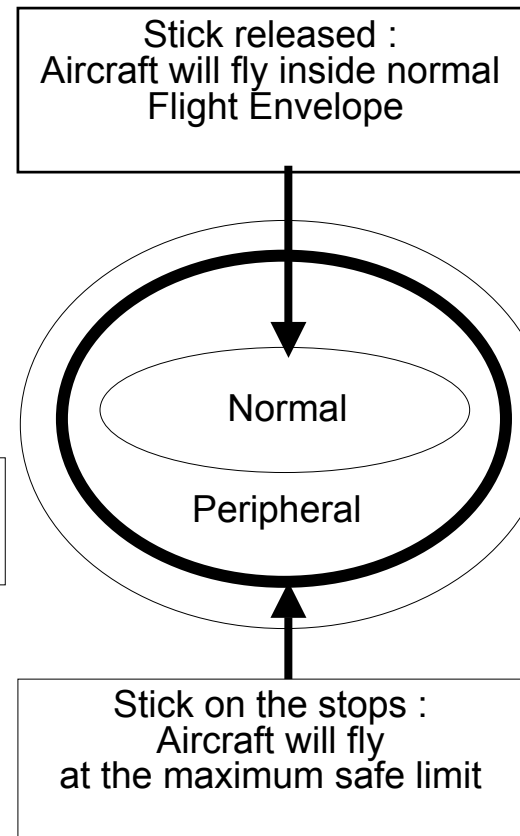
DECISION HELP

- 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



FLY-BY-WIRE DEPENDABILITY

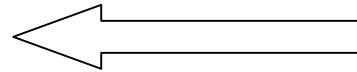
- Some lessons

- ▶ 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

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
- Potential trends for Fly-by-Wire



POTENTIAL TRENDS

- Genericity – standardisation
 - ▶ Reduced cost, development & recurring
 - ▶ But, common point of failure
- Mechatronics
- “smart” structure
- “Large” networking
- Formal methods / test
- simulation

THANK YOU – QUESTIONS?

Reference: Traverse, P., Lacaze, I., Souyris, J.: Airbus fly-by-wire: a total approach to dependability. 18th IFIP World Computer Congress – Topical session “fault tolerance for trustworthy and dependable information infrastructure” (Toulouse, France), Kluwer Academic Press, 2004, pp.191-212.



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**