

---

# Nouvelles architectures avioniques

## Sûreté de fonctionnement

**Pascal Traverse**

1. Principes
2. Architecture

---

1. Principes

2. Architecture avionique A380

Commandes de vol électriques

- disponibilité
- mouvement intempestif de gouvernes

---

## system failures

- control and monitoring computers
- components redundancy
- challenges & trends

## design and manufacturing errors

- error avoidance
- error tolerance
- challenges & trends

## particular risks

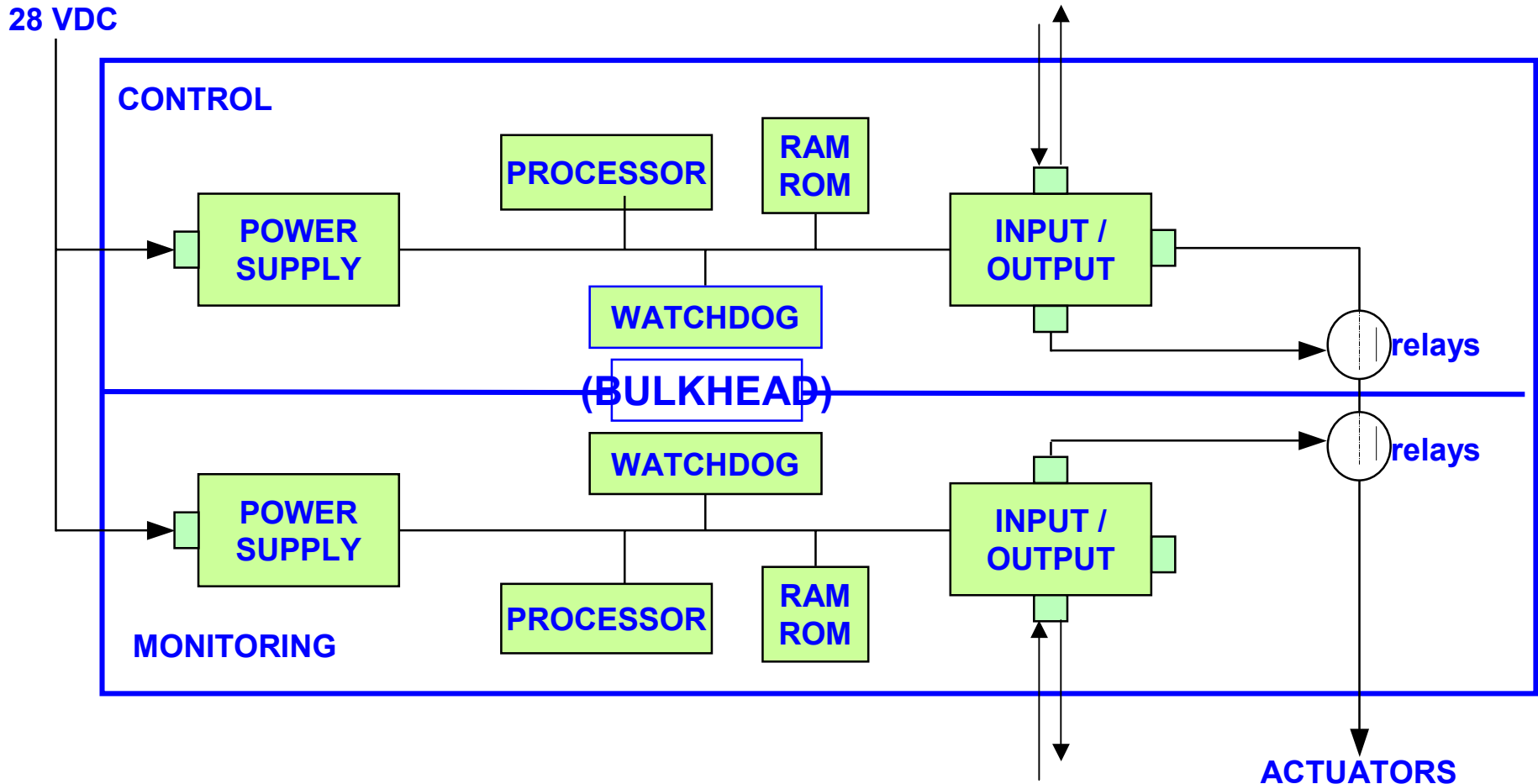
- segregation
- ultimate back-up
- challenges & trends

## man-machine interface

- flight envelope protection
- maintenability
- challenges & trends

# system failures

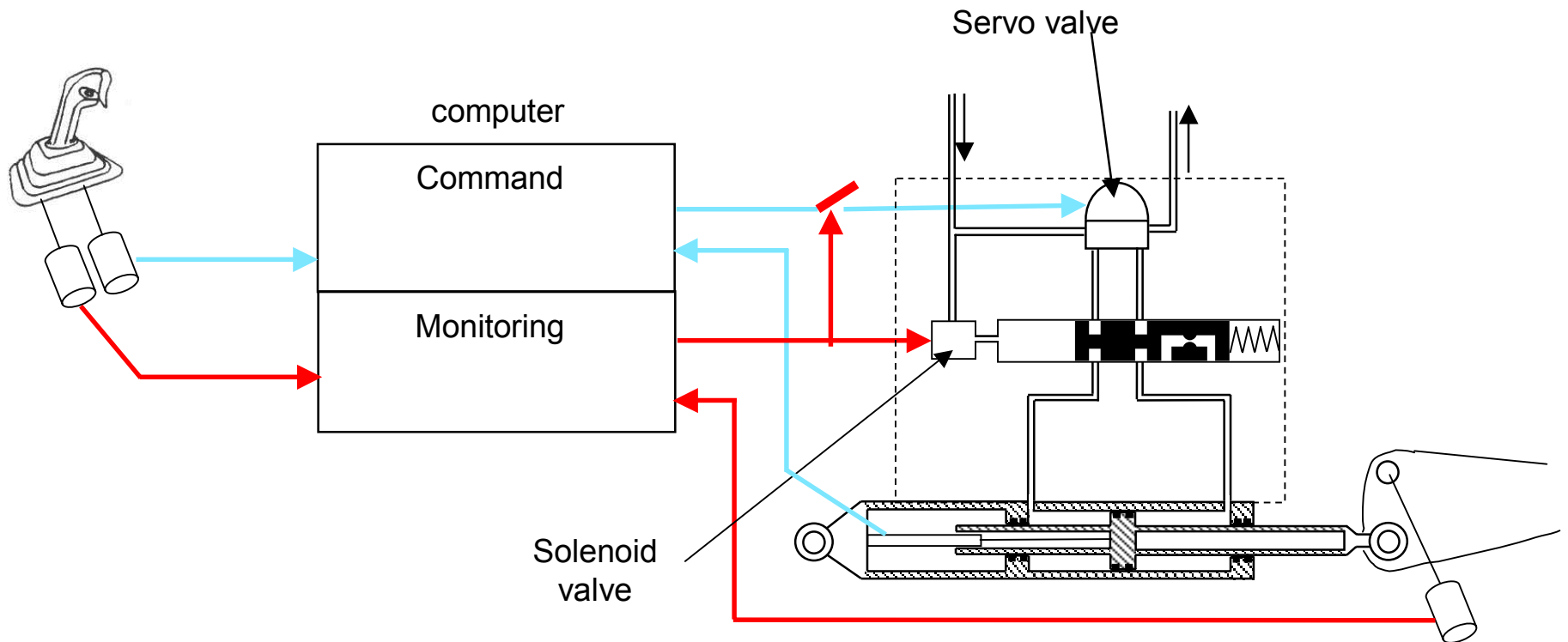
- control and monitoring computers



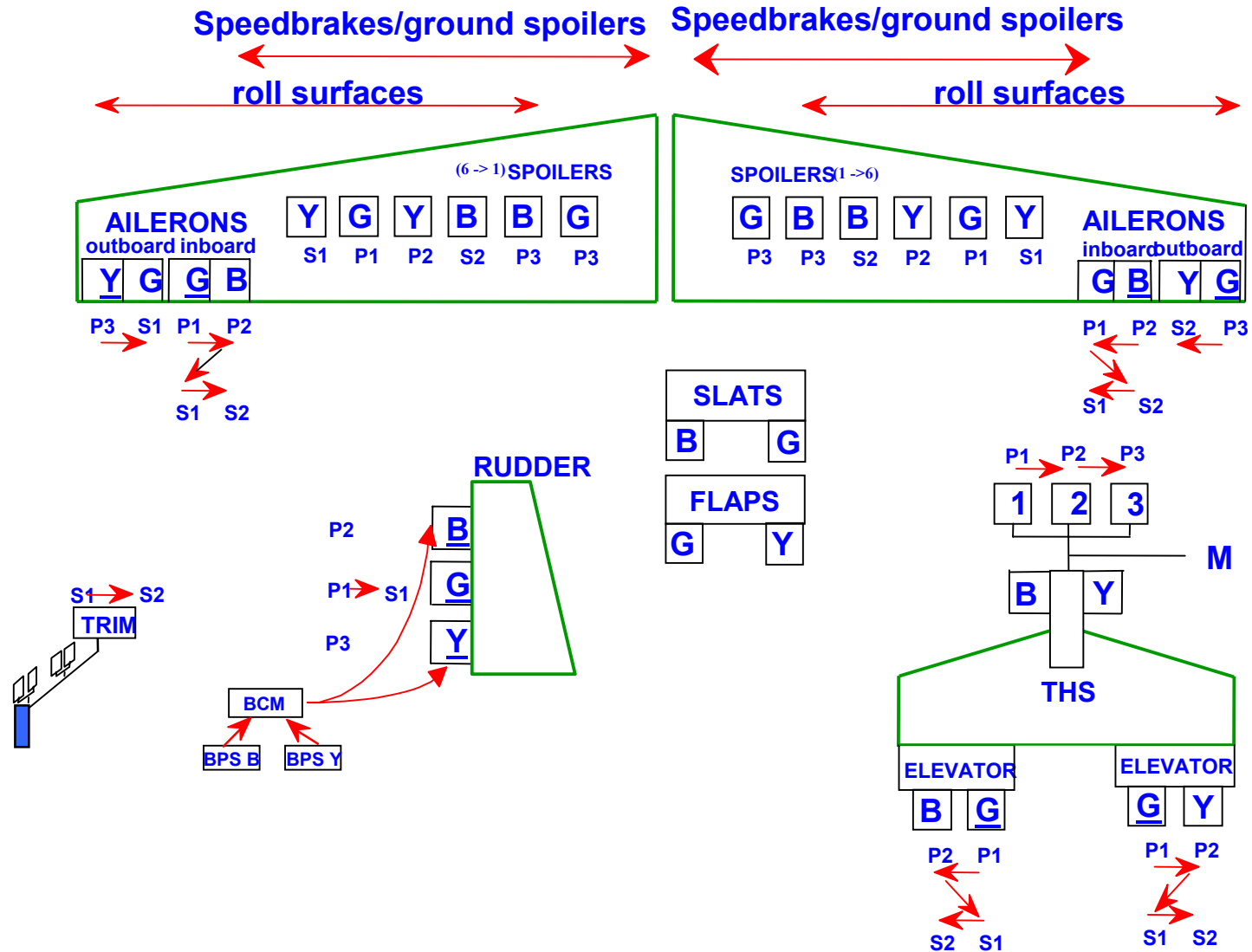
■ Lightning strike protections

# system failures

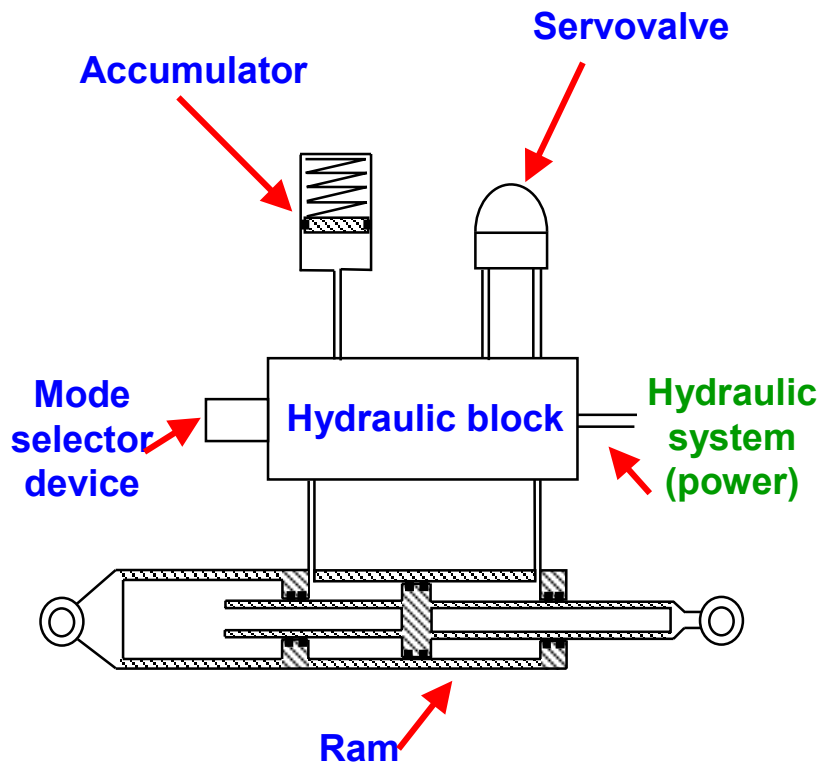
- control and monitoring computers



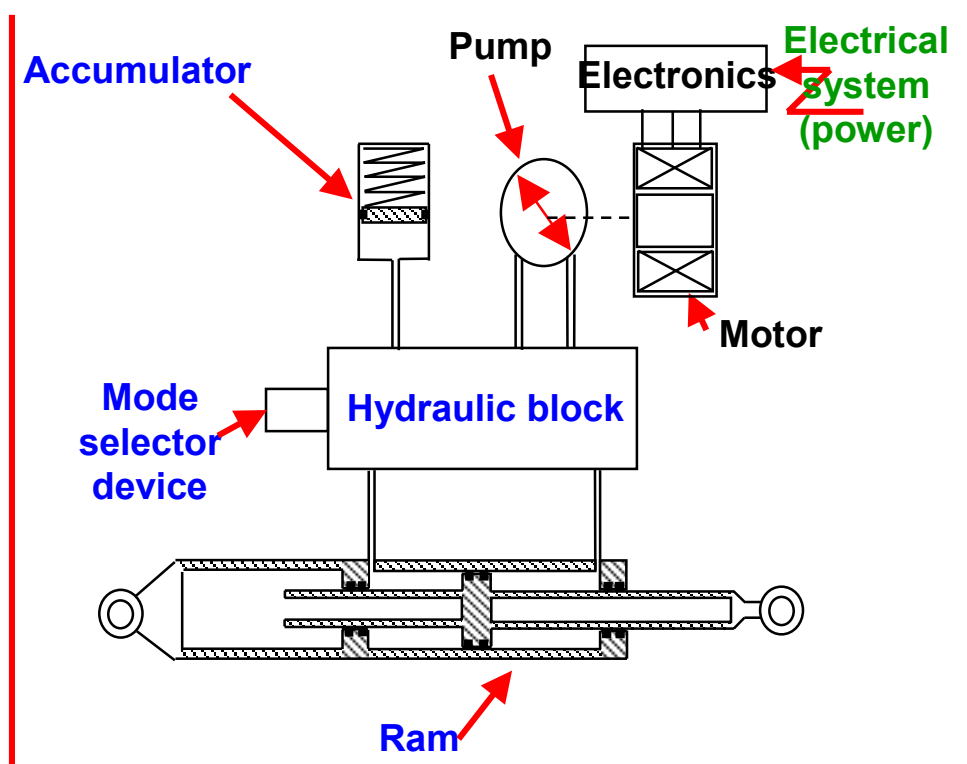
- components redundancy



- components redundancy



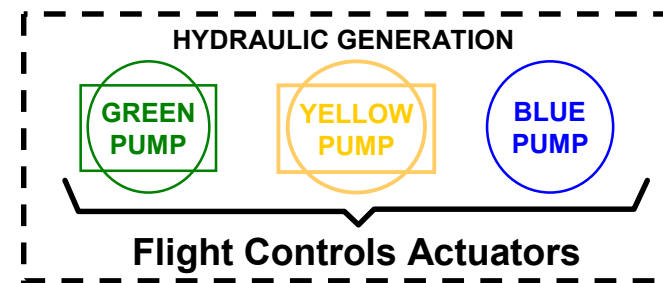
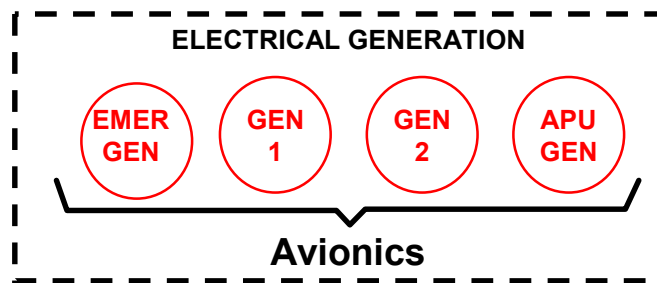
**HYDRAULIC SERVOCONTROL**



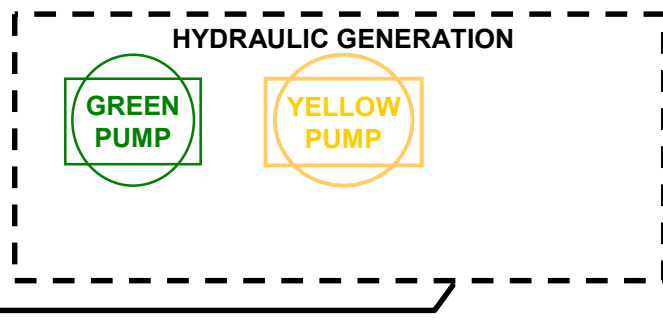
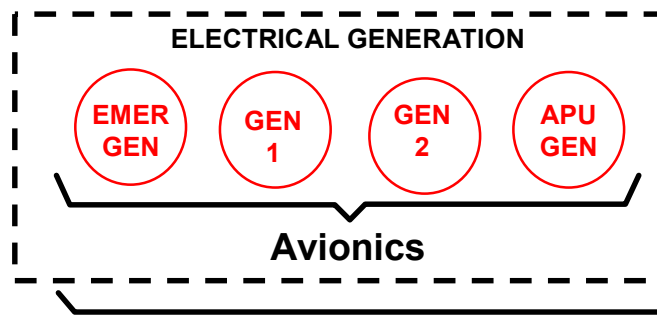
**ELECTRO-HYDROSTATIC ACTUATOR**

- components redundancy

• **A320 ... A340**



• **A380 A400M**



Flight Controls Actuators



# system failures

---

- challenges & trends

EHA are a great opportunity (weight, dissimilarity, segregation) and a challenge with new failure modes

# design and manufacturing errors

Airbus Fly-by-Wire:  
system is developed to ARP 4754 level A  
Computers to DO178B & DO254 level A

Error avoidance

Two types of dissimilar computers are used

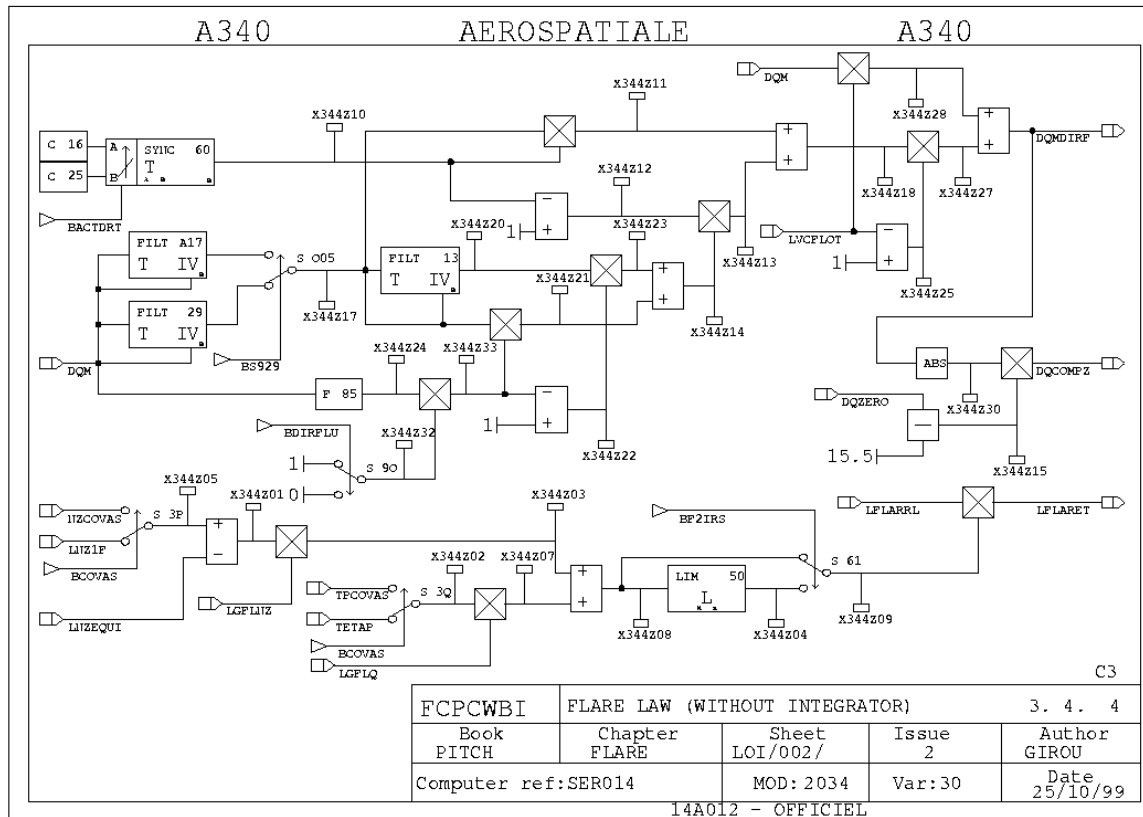
PRIM  $\neq$  SEC

Error tolerance



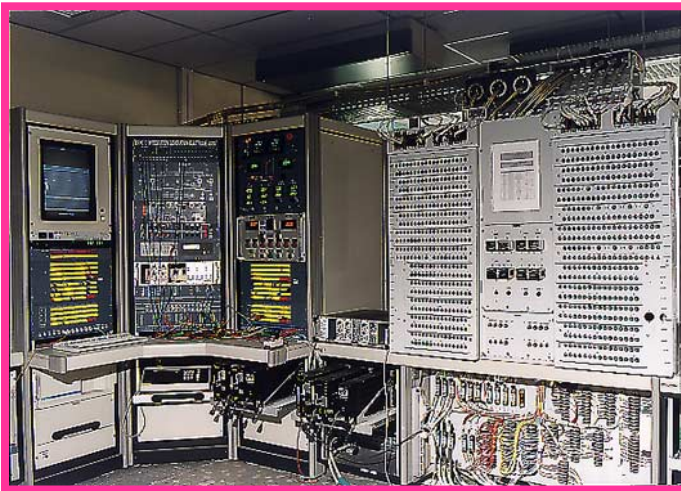
# design and manufacturing errors

- error avoidance



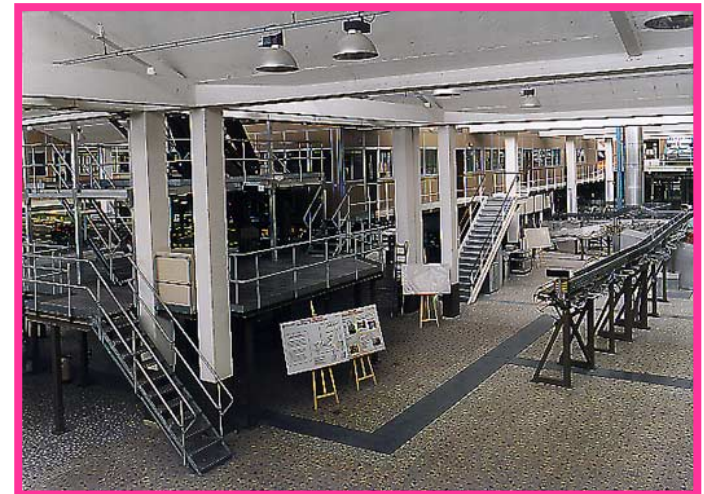
- formalised specification (SAO/SCADE)
- automatic programming

- error avoidance

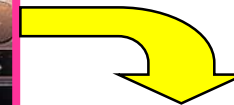


Bench for system integration

SAO/SCADE automatic programming



Iron Bird



Simulator  
•full cockpit  
•desktop

# design and manufacturing errors

---

- error tolerance

ELAC  $\neq$  SEC

PRIM  $\neq$  SEC

$\Rightarrow$  4 different softwares

COM  $\neq$  MON

data diversity

with EHA  $\Rightarrow$  electrical power AND hydraulic power

# design and manufacturing errors

---

- challenges & trends

PRIM / SEC dissimilarity: from random to managed dissimilarity

in-service experience: dissimilarity for system availability is essential

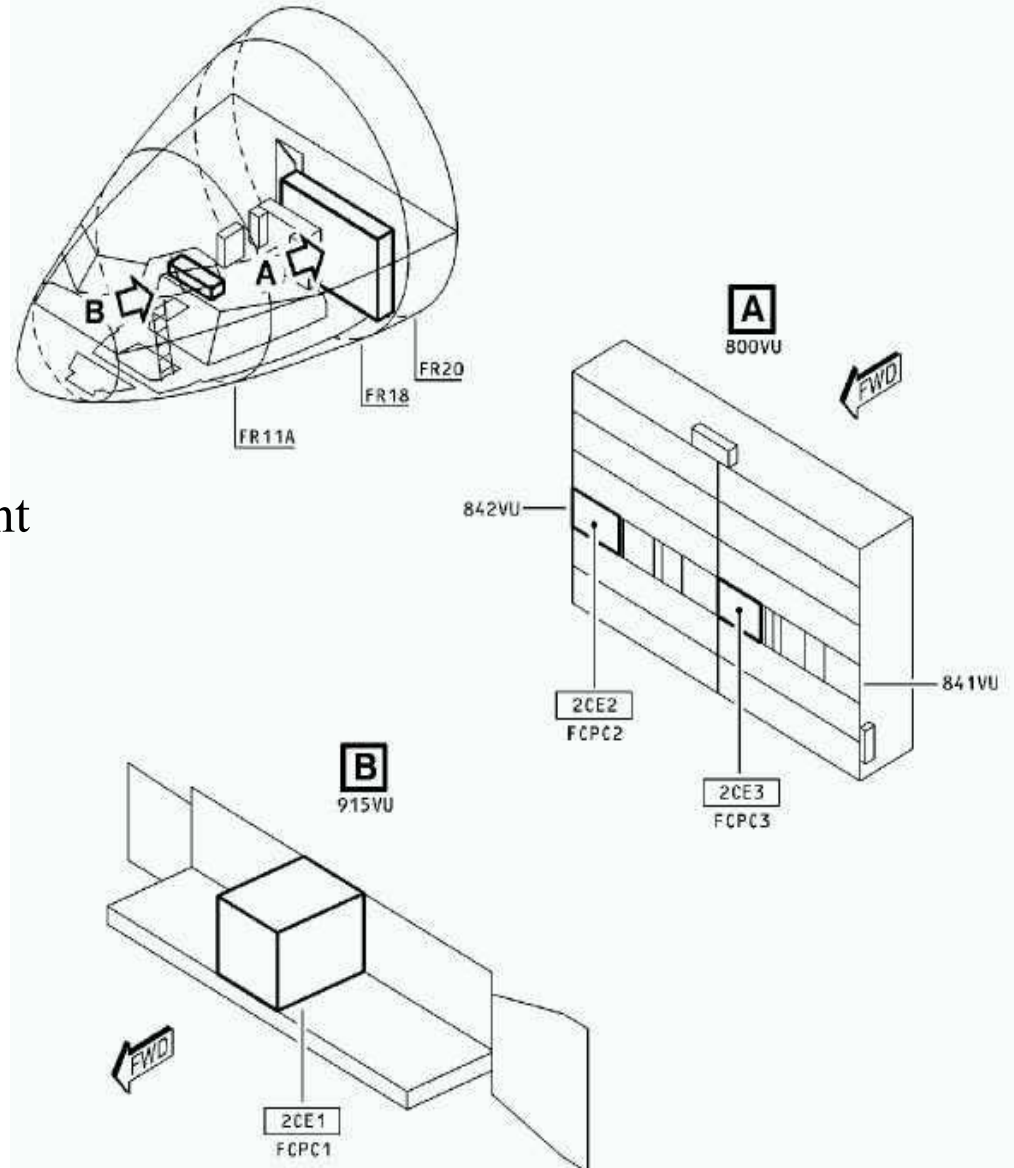
# particular risks

# Computers separation

- segregation

avoidance of a common failure point

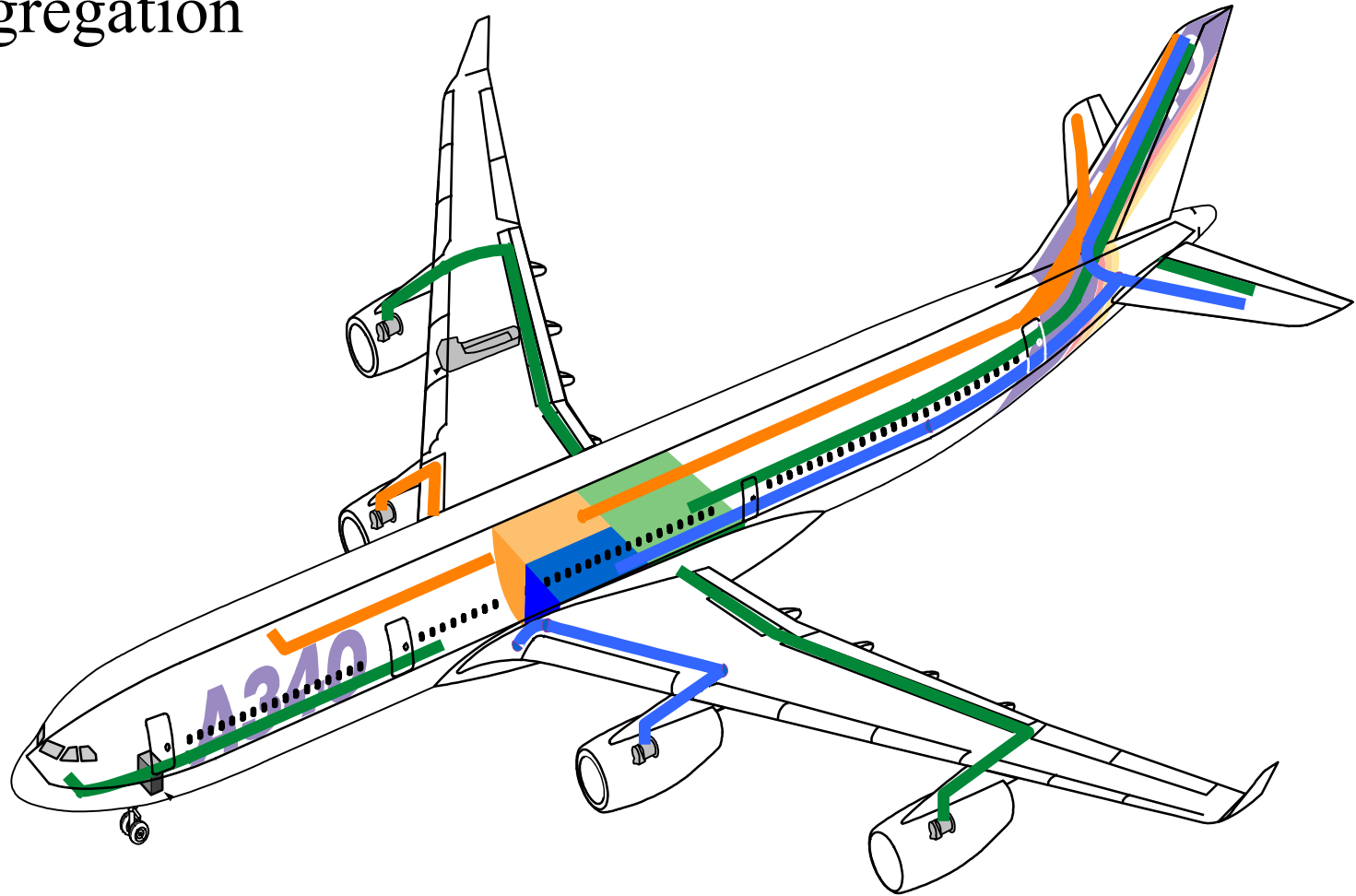
- loose luggages
- spilling liquid
- ...



# particular risks

# Power sources separation

- segregation



A380, A400M: increased segregation thanks to EHA



- ultimate back-up

goal of Airbus ultimate back-up:

continued safe flight while crew restore primary flight controls

- reset PRIM and SEC
- reset electrical generation

use of ultimate back-up designed to be Extremely Improbable

no credit in certification

- ultimate back-up

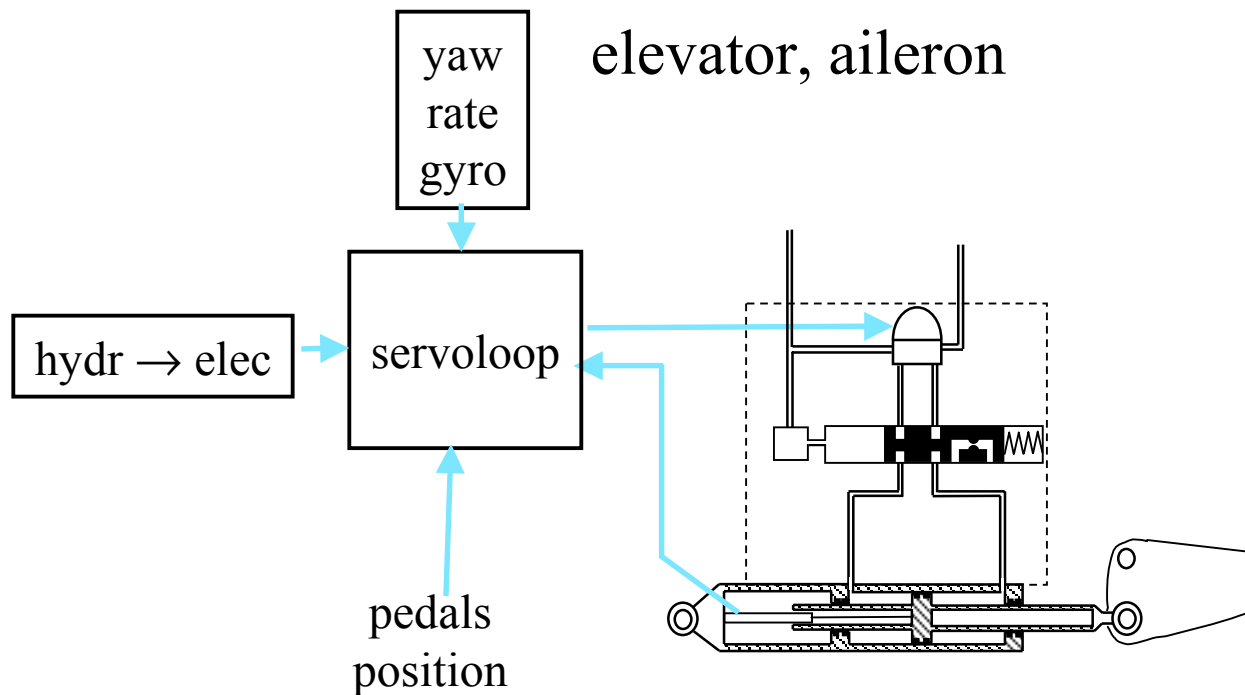
A320: mechanical linkage to THS & rudder

A340: ditto, plus Back-up Yaw Damping

A340-600: mechanical linkage to THS

autonomous, electrical back-up from pedals to rudder

A380 A400M: electrical back-up on rudder,  
elevators, ailerons



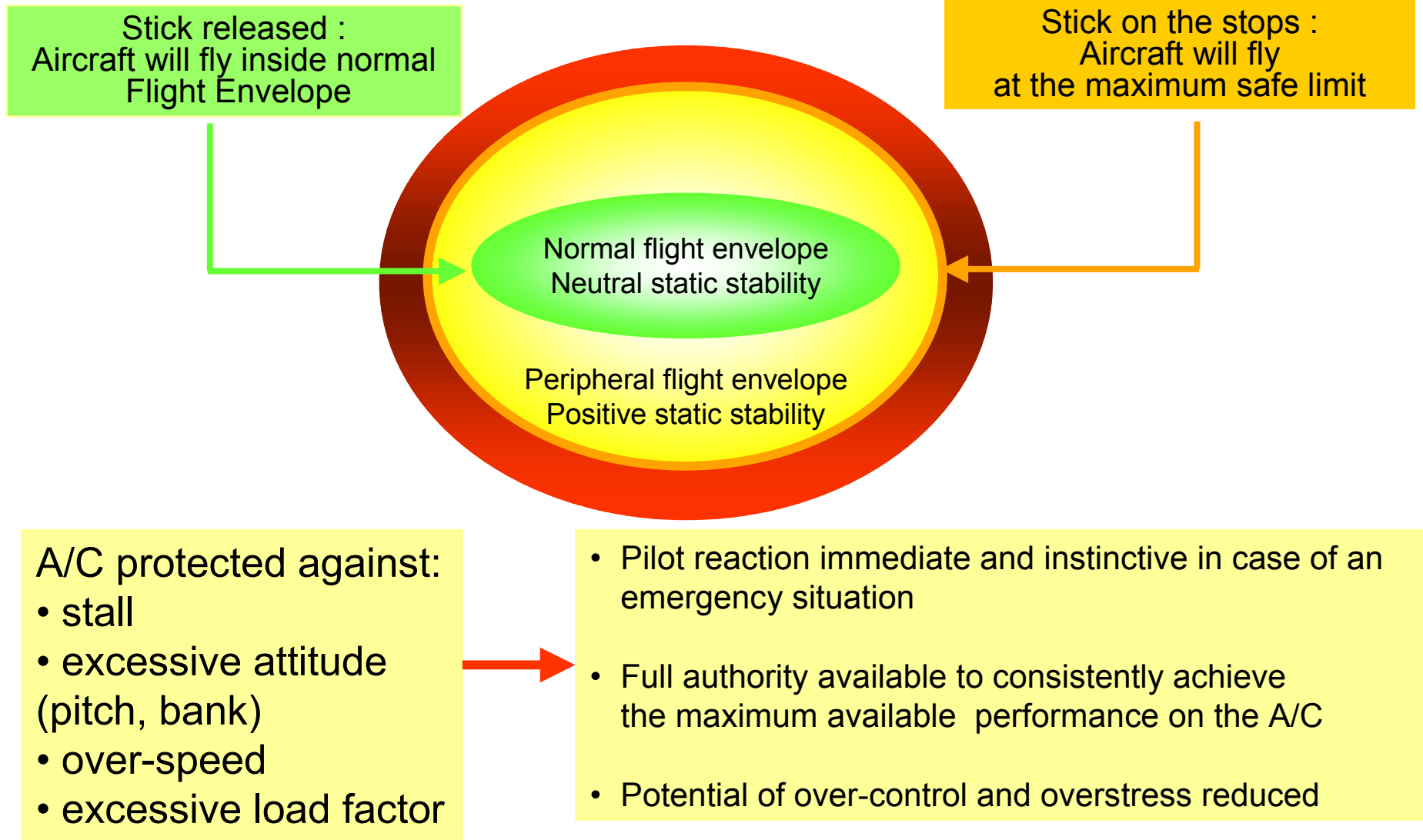
## particular risks

---

- challenges & trends
  
- military environment on A400M
  
- A340-600 Taxi Aid Camera System:  
open the way to affordable, maintainable flight-by-light

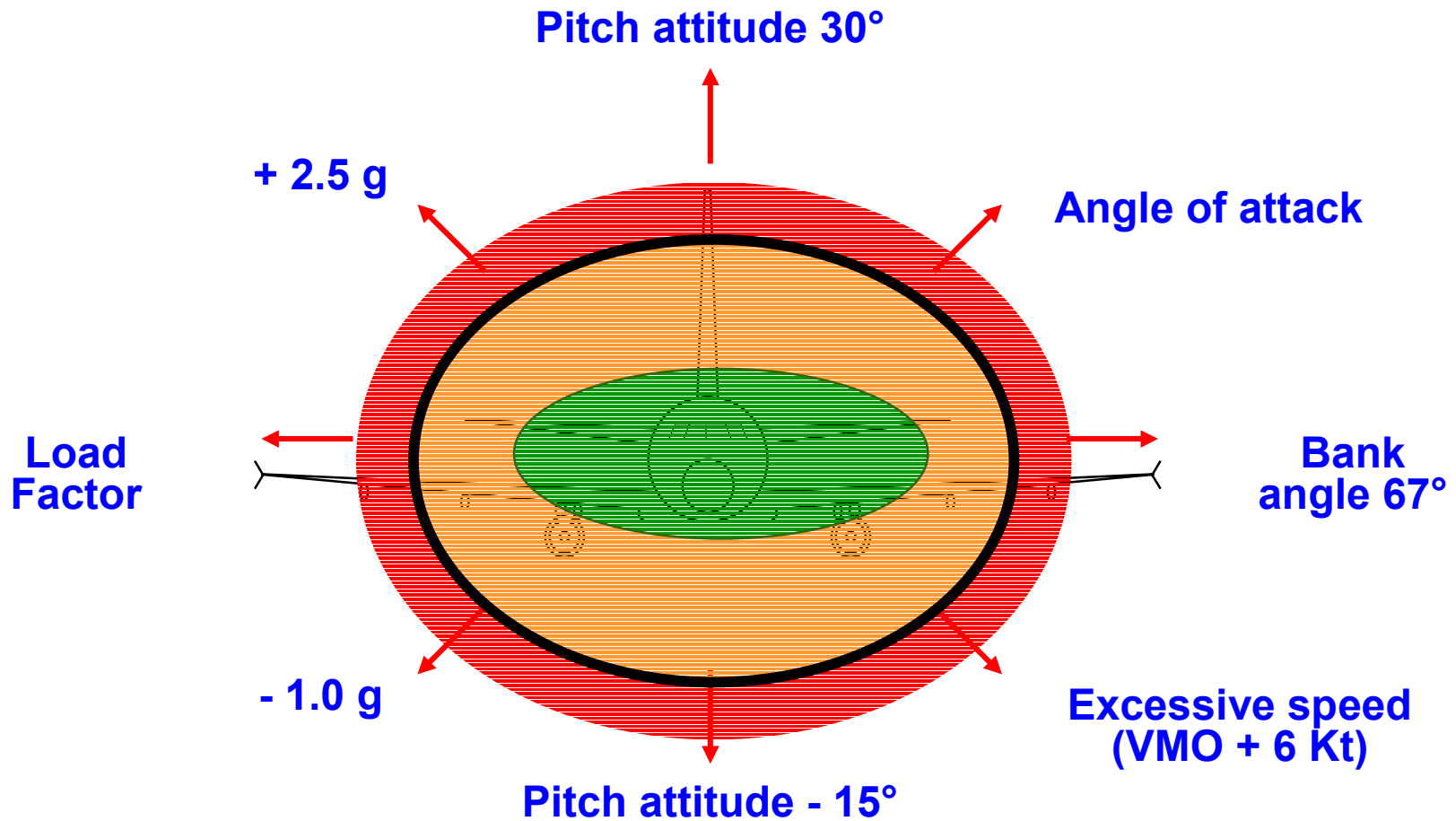
# man-machine interface

## •flight envelope protection



# man-machine interface

- flight envelope protection



# man-machine interface

---

- maintenability

- extensive fool-proofing

- precise trouble shooting

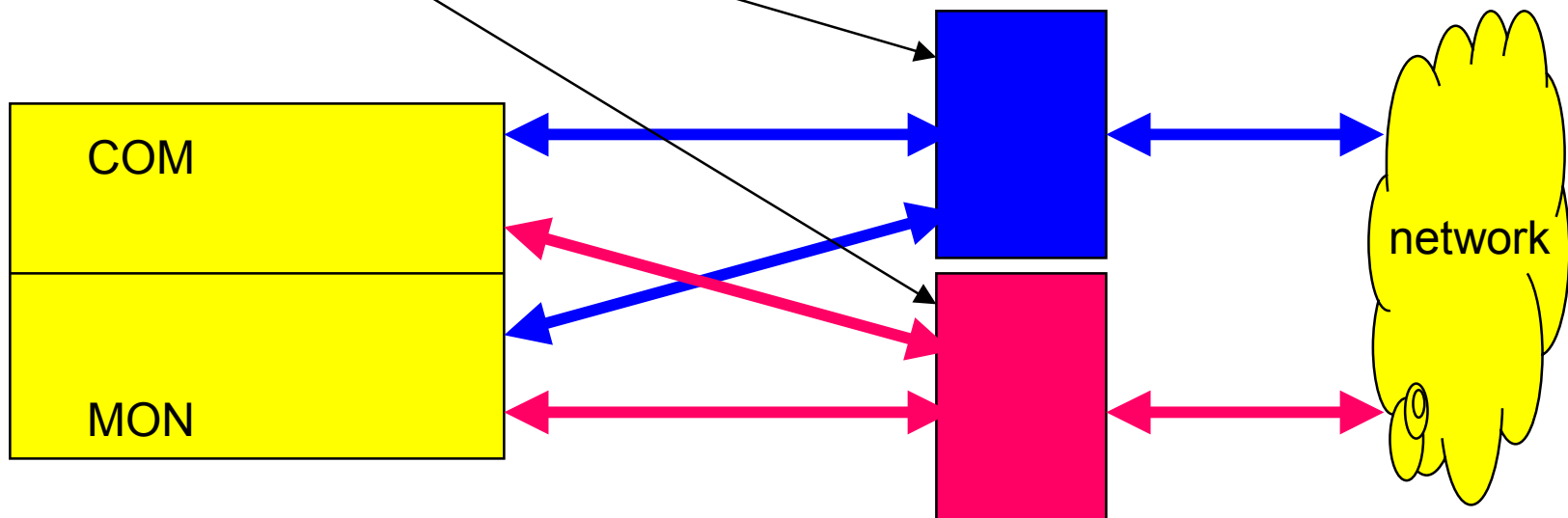
- (800 different failure diagnostic)

- challenges and trends

- maturity at entry into service

# A380 Aircraft Data Communication Network

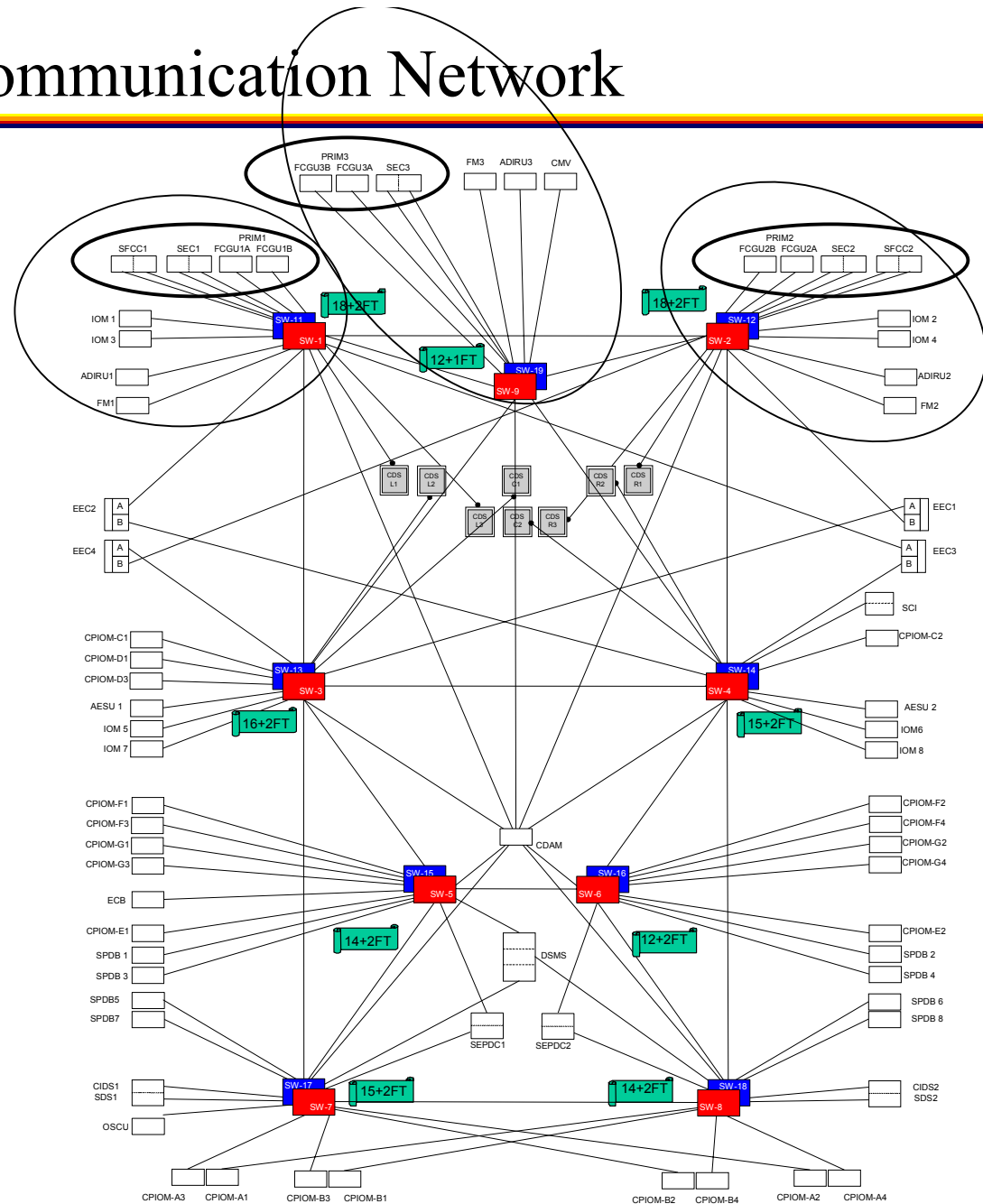
- dual redundant network
- Switched Ethernet type



# A380 Aircraft Data Communication Network

Usual electrical separation of blocks of computers

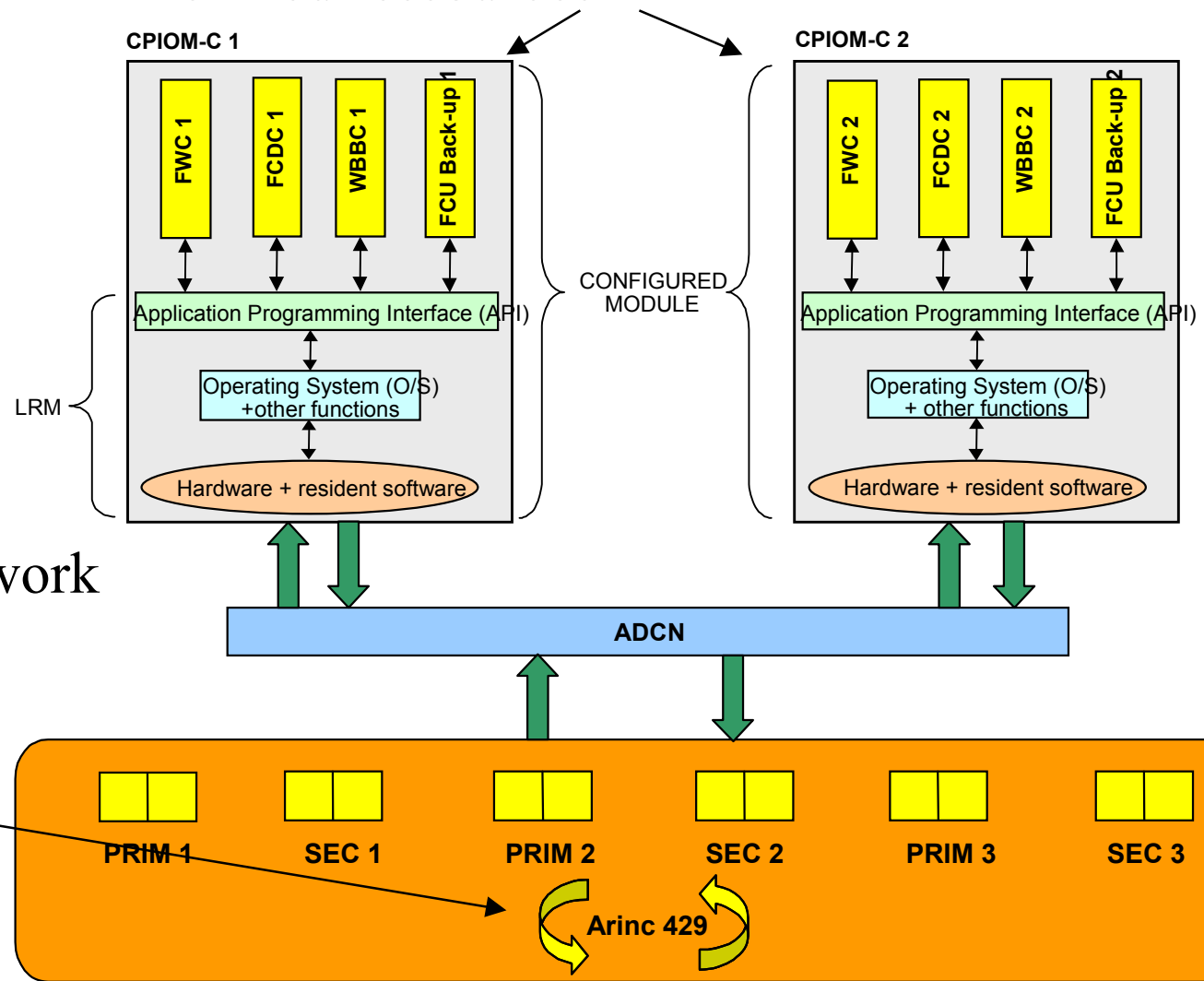
loss of ADCN /  
mutated data  
on network:  
not critical





# A380 ADCN & SHARED RESSOURCES

non essential functions (warning, maintenance, ...) located on shared reSSources



Essential data network  
-old technology  
-Separated from  
ADCN

