GEA Tianjin / 中国民航大学中欧航空工程师学院

SB 503 - Avionics Technologies

1- introduction to Avionics Technologies

1-1 Introduction to Safety & Systems

1-2 Avionics Certification Process including applicable Standards

1-3 Human Factors Prospectives

1-4 Avionics System Architectures (Logical- Functional)

1-5 Avionics Systems & [Missions- Functions - Resources]

Professor: H. GOUTELARD (Contractor ENAC/ Sup'Aéro)
Thales Avionics

Agenda

- Avionics Systems general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ Candidate logical architectures
- Architecture building examples
  - Display primary parameters

GEA Tianjin / 中国民航大学中欧航空工程师学院

The Aircraft is a node of the Airliner "IT System"

Controlled			*Uncontrolled*
Airframer	*Airline*		*Passenger*
CLOSED	*PRIVATE*		*PUBLIC*
Control the Aircraft	*Operate the Aircraft*	*Inform and Entertain the Passengers*	
Aircraft Control Domain (ACD)	**Airline Information Services Domain (AISD)**	**Passenger Information And Entertainment Services Domain (PIESD)**	**Passenger-owned Devices (POD)**
Flight and Embedded Control Systems	Administrative Functions	In-Flight Entertainment	Computing Devices
Cabin Core Systems	Flight Support	Passenger Internet	Wireless Devices (Cellular, PDAs)
	Cabin Support	On-board Web Access	:
	Maintenance Support	Passenger Device Interface	Gaming Devices
Air-Ground Network Interface	Air-Ground Network Interface	Air-Ground Network Interface	
VHF / HF / SATCOM	Wireless LAN	Broadband / Cellular	

Security
Responsibility
Airline Ops
Missions
Domains

View Points

Aircraft Overview - Operations (AEEC-ARINC Ref. Model)

Air-Ground Datalink Services (e.g., ACARS)

Airport Network (e.g., Gatelink)

Air-Ground Broadband Network (e.g., INMARSAT)

Com. Means

Air Traffic Service Providers	**Airline**	**Airline-Approved 3rd Party Providers**	**Passenger-accessed 3rd Party Providers**

Reference

GEA Tianjin / 中国民航大学中欧航空工程师学院

On Board Systems breakdown

Flight Controls

Avionics (Mission Management)

- ATA 21 & 36 Air Systems
- ATA 22 Auto Flight System (AFS)
- ATA 23 Communication
- ATA 24 Electrical System
- ATA 26 Fire and Smoke Protection
- ATA 27 Flight Controls
- ATA 27 Slats and Flaps
- ATA 28 Fuel System
- ATA 29 Hydraulic System
- ATA 30 Ice and Rain Protection
- ATA 31 Indicating/Recording Systems
- ATA 32 Landing Gear
- ATA 34 Navigation
- ATA 35 Oxygen
- ATA 42 Avionics Networks and IMA
- ATA 45 Onboard Maintenance System (OMS)
- ATA 46 Information Systems
- ATA 49 Auxiliary Power Unit (APU)
- ATA 70 Engines

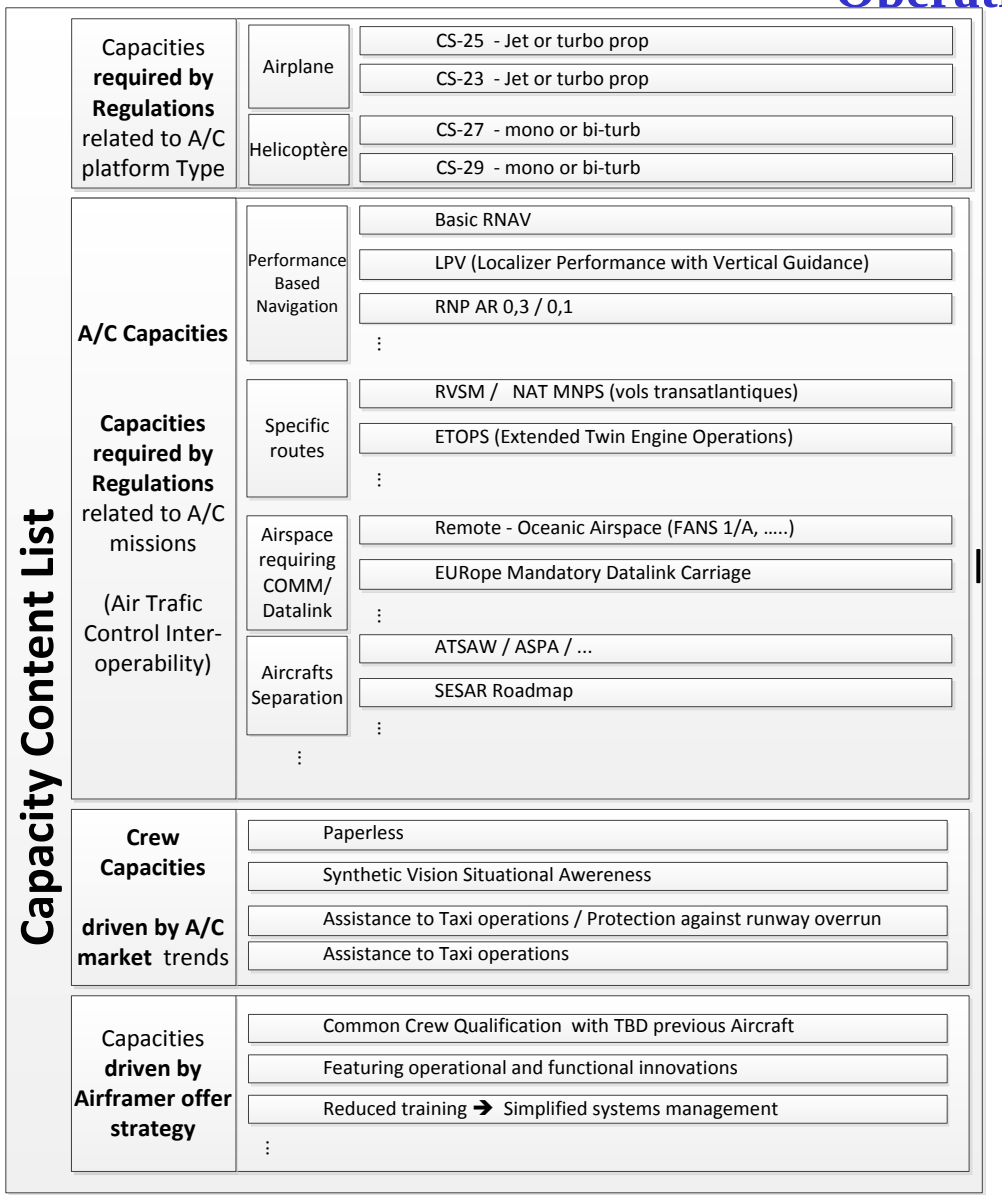
Aircraft systems Management

- **Or utilities**
- **Or Auxillary systems**

Engine systems

4 Domains: Flight Controls, Avionics, A/C Systems, Engines Systems

Operational Capacities



For each market segment

- **A/C type regulations compliance**
  - Helico, Turbo prop, Jet
  - Pax seats ➔ Single / dual pilots
- **A/C capacities (A/C missions)**
  - Driven by ATC interoperability or imperative A/C capacities
  - Operations regulations
- **Crew capacities (market trends)**
  - Options becoming standards
  - Mission Management efficiency
  - Situational awareness
- **Airframer choices**
  - Cross Crew Qualification
  - Innovative cockpit

Method Steps

Method Contents

- Customer Operational Need Analysis

  What **the users** of the system have to accomplish

  ORD/OCD
  CONOPS

- System/SW Need Analysis

  What **the system** has to accomplish for the Users

  SSS

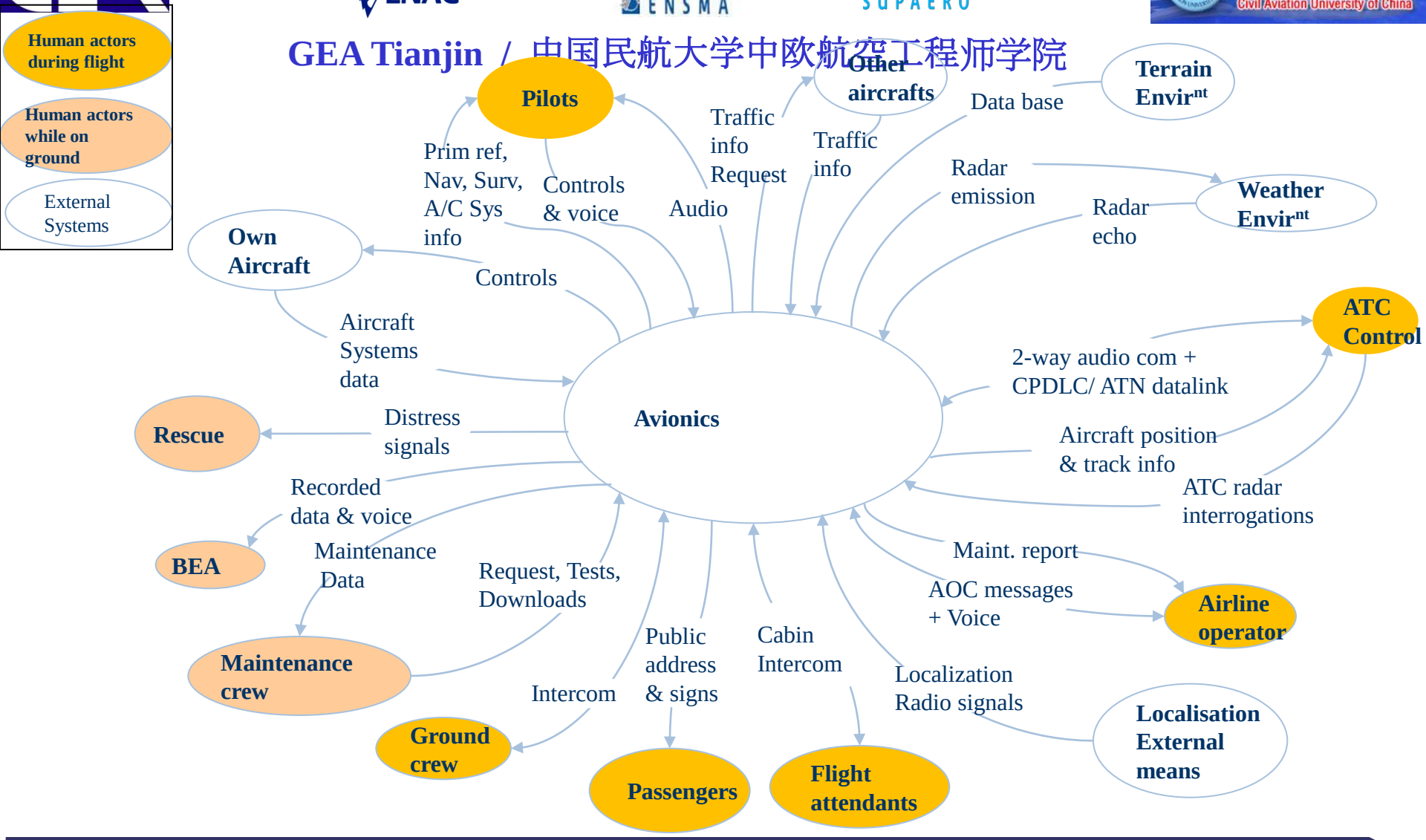
- Logical Architecture design

  How the system will work so as to fulfil expectations

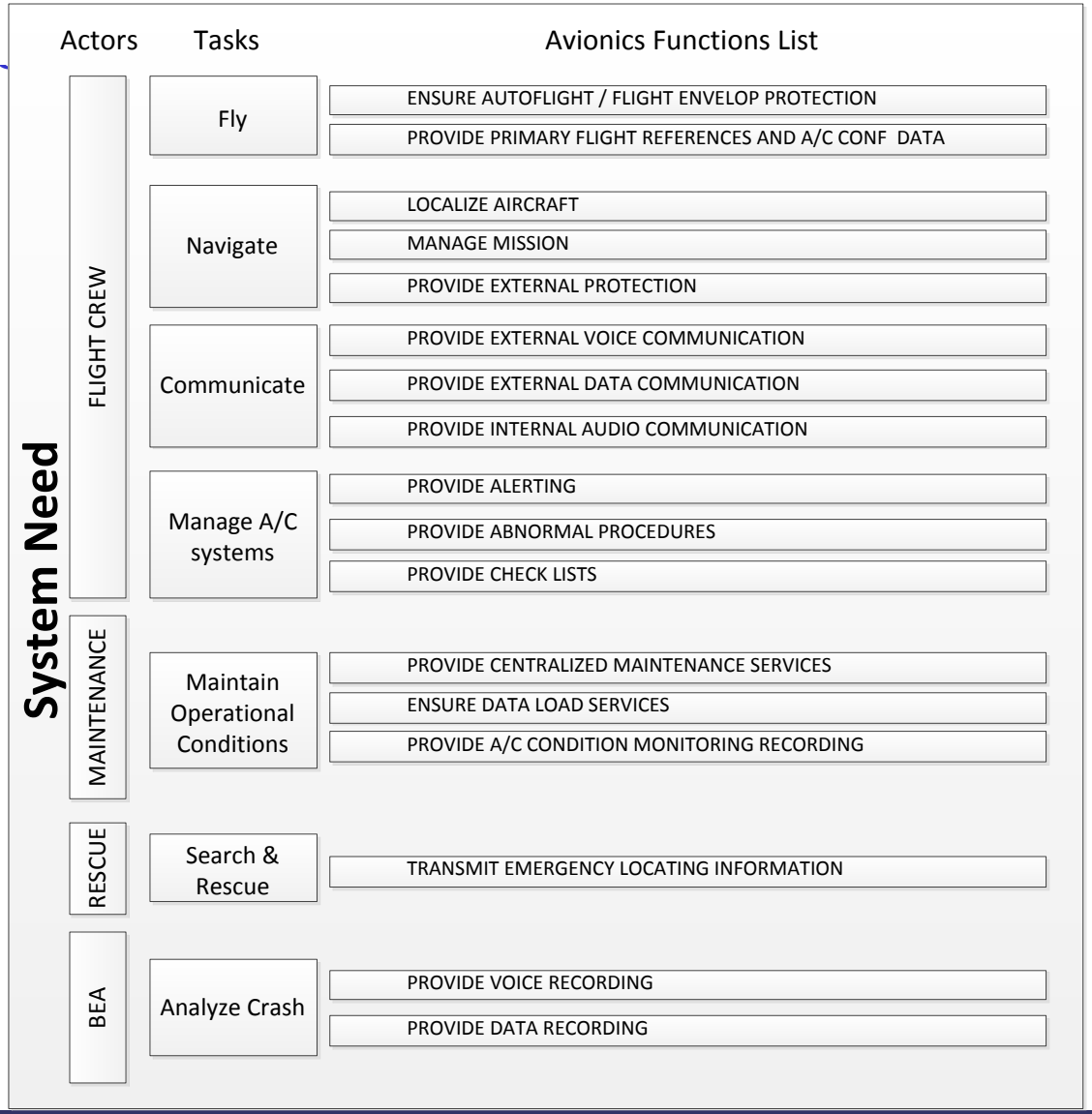
  SSDD

- Physical Architecture design

  How the system will be developed & built



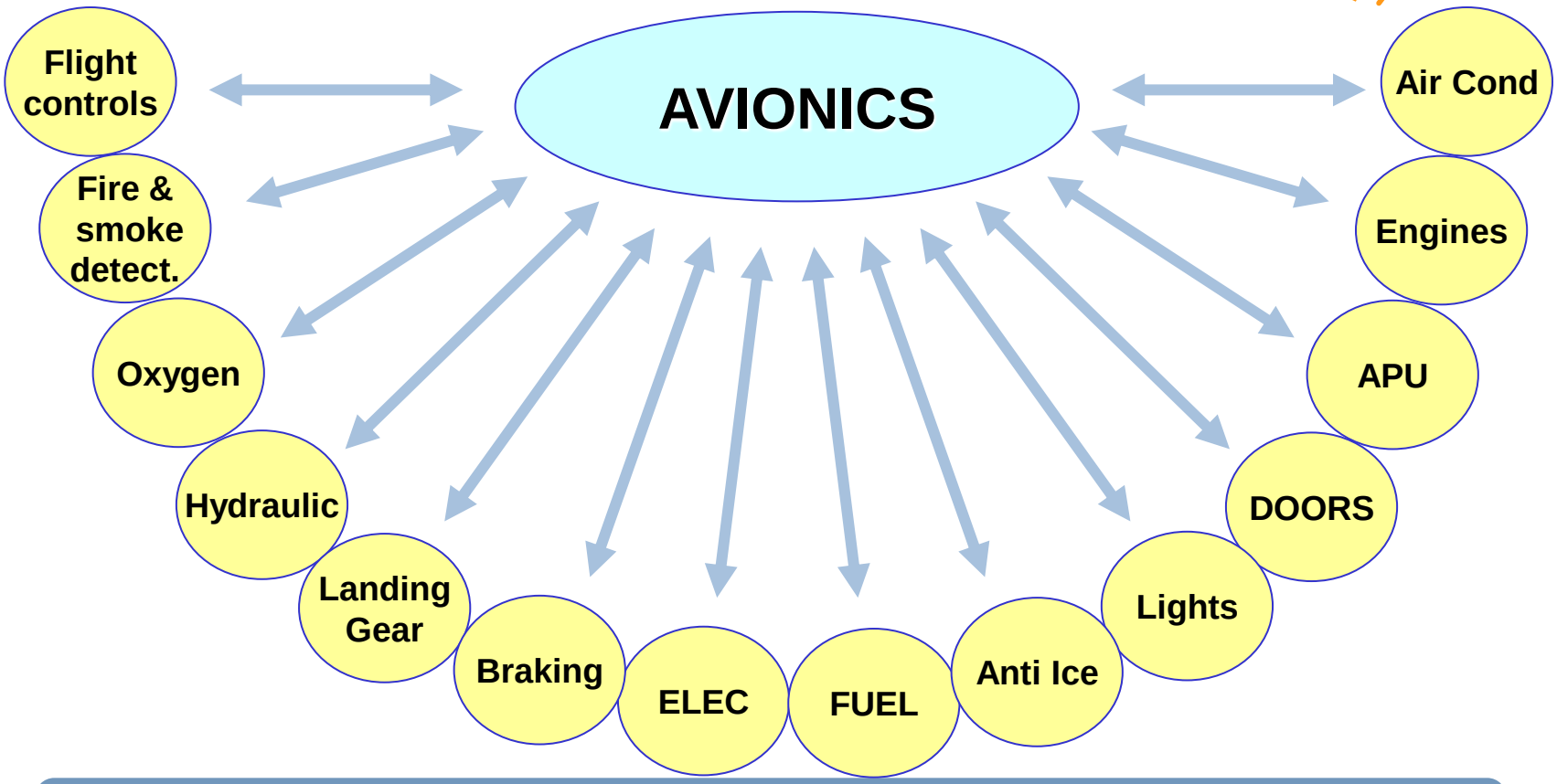
Avionics Systems serves one or several user(s)



Each of the functions provides a service for one or several user(s)

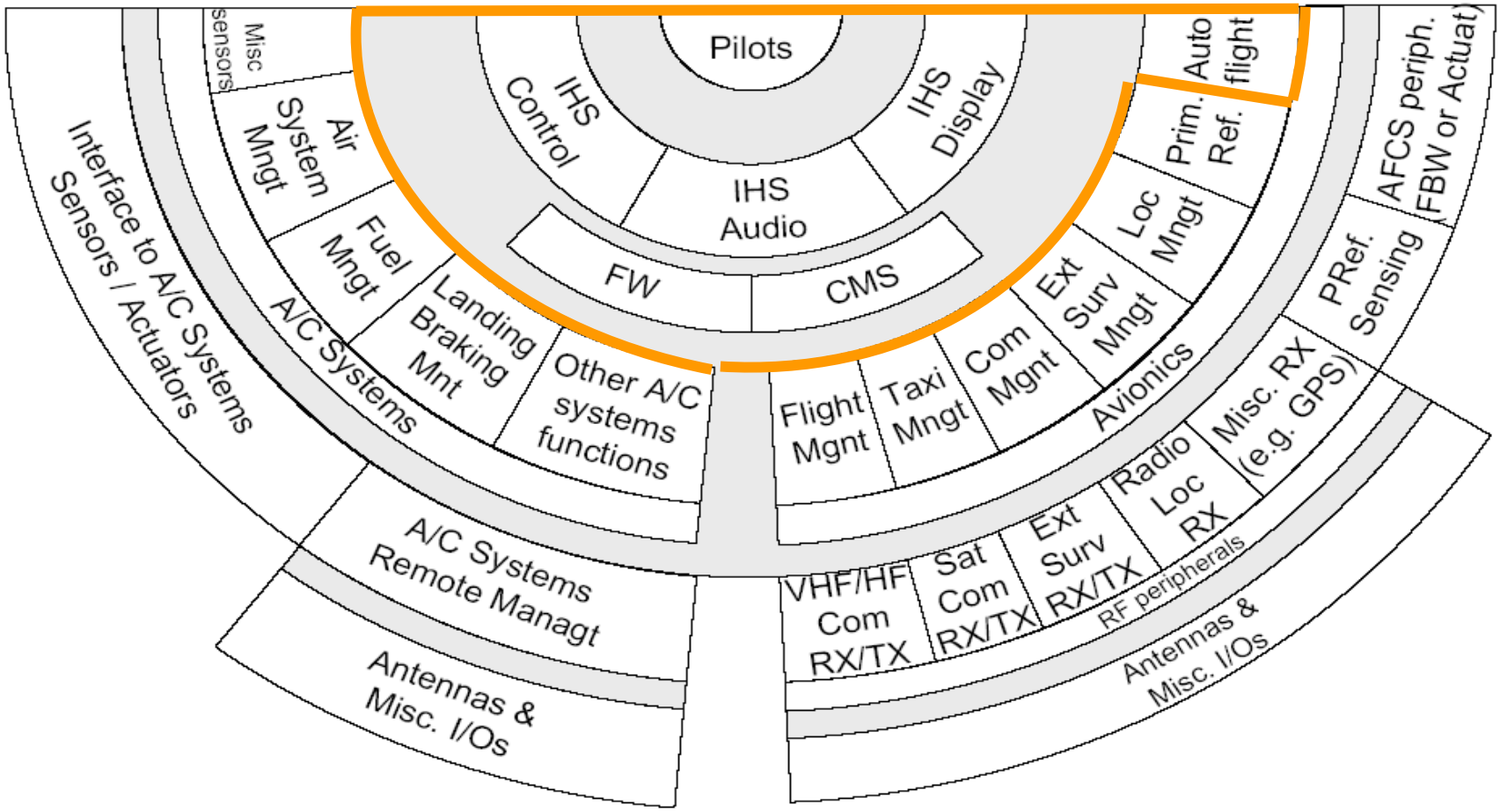
GEA Tianjin / 中国民航大学中欧航空工程师学院

Avionics and A/C systems

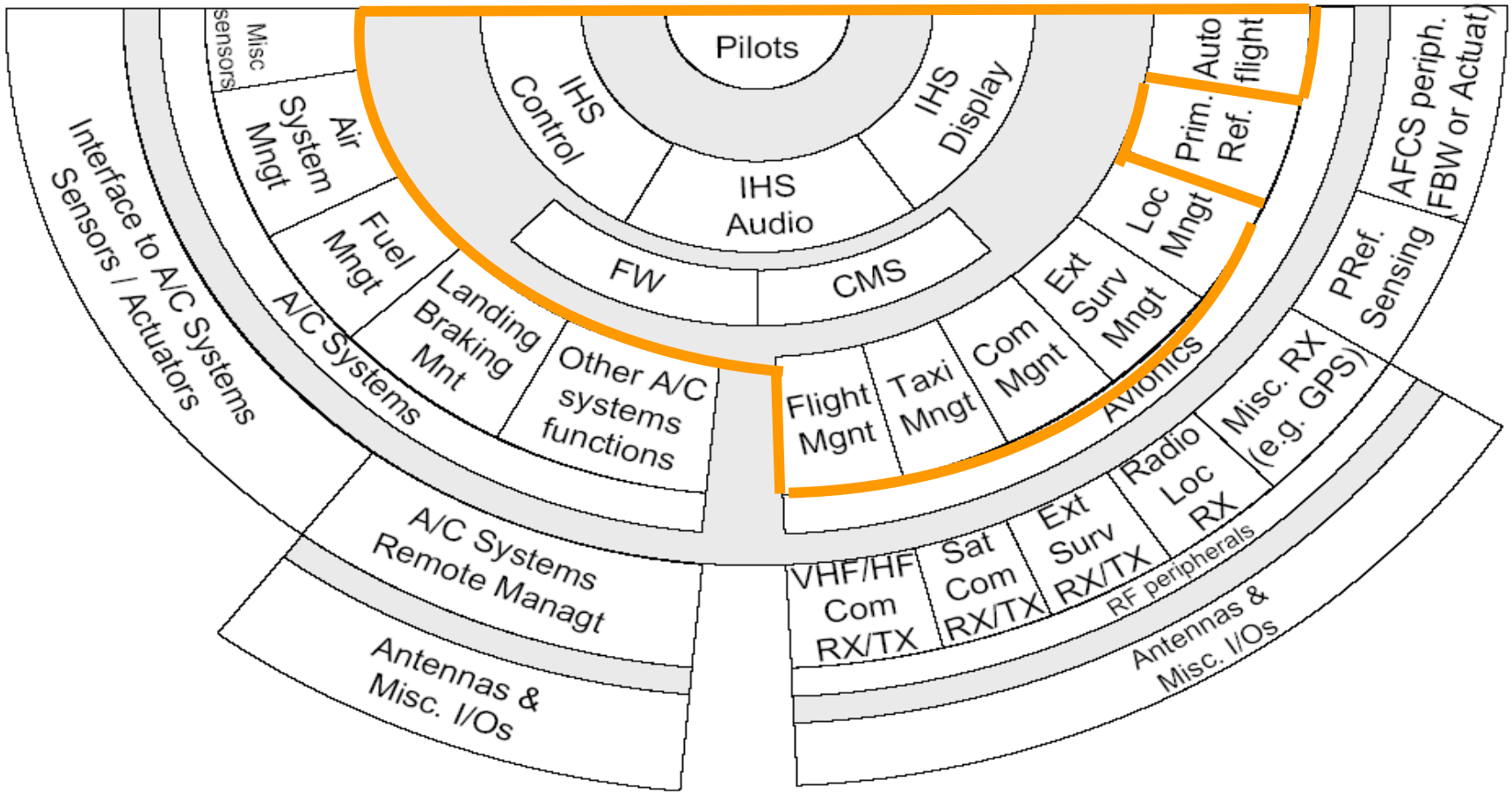


Mastering A/C interfaces is the perequisite to Master an Avionics System

Core Avionics Platform External ICD- Ex: Pgr1

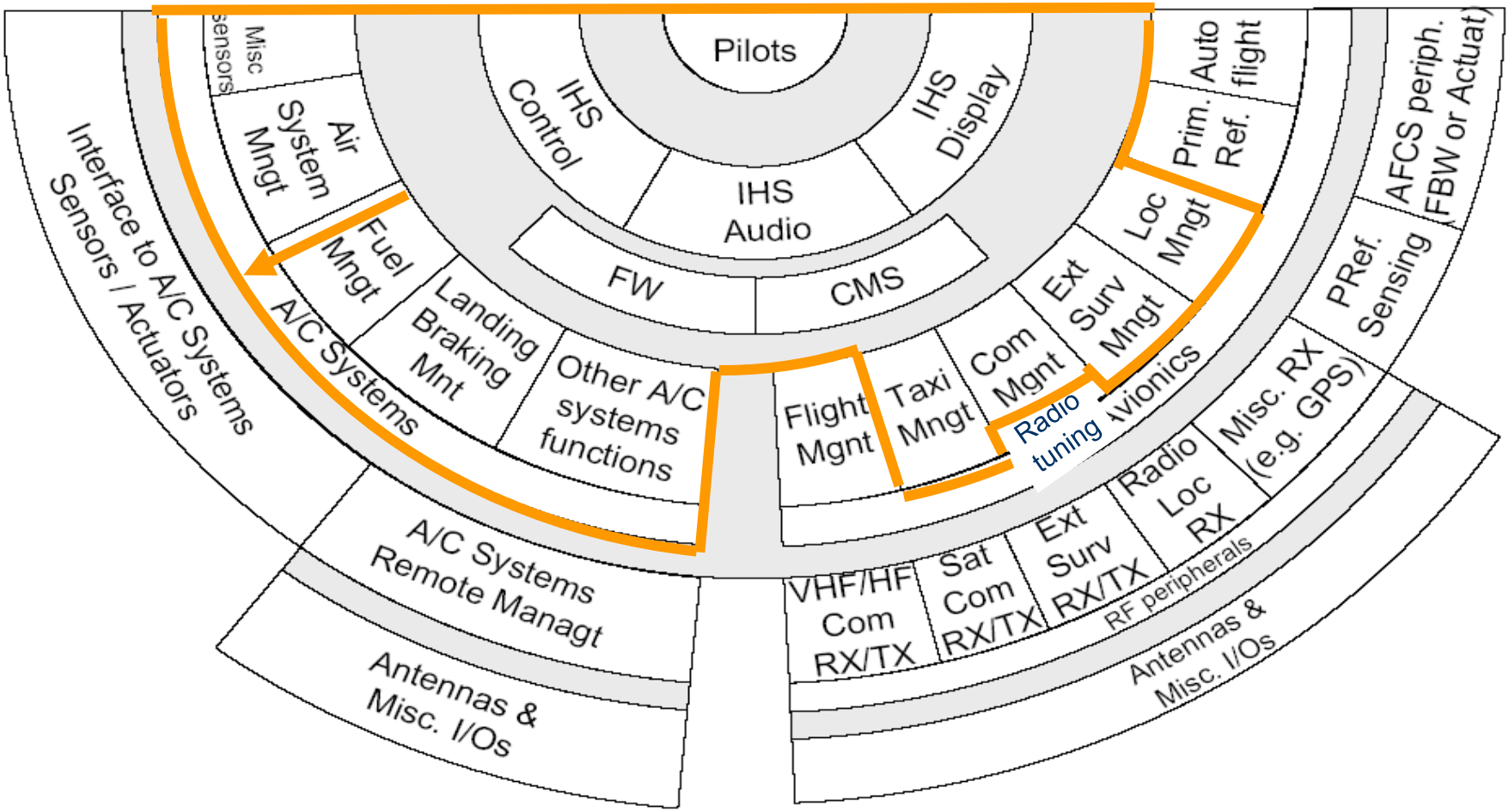


Core Avionics Platform – ICD Ex: Pgr2



GEA Tianjin / 中国民航大学中欧航空工程师学院

Avionics + Utilities – ICD with Integrated Utilities (Ex: Pgr3)



Agenda

- Avionics suite general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ candidate logical architectures
- Architecture building examples
  - Display primary parameters

中国民航大学中欧航空工程师学院

Architecture Development Process (1/2)

AirFramer

AF

Aircraft Needs

AirFramer Perimeter

Aircraft Certification

ATA42

IMA System (ATA 42) Perimeter

System Designer

SD

Syst Architecture

Syst Integration & Qualification

IMA System Architecture

Resource Allocation

IMA System Integration

Function Supplier

FS

Function Design

Platform Requirements

Configuration Qualification

Function Qualification

Platform Design

Platform Qualification

PS

Platform Development

Function supplier Perimeter

PF supplier Perimeter

Function Development

Mature innovative engineering process based on Early Validation Engineering Simulators, & Test environment

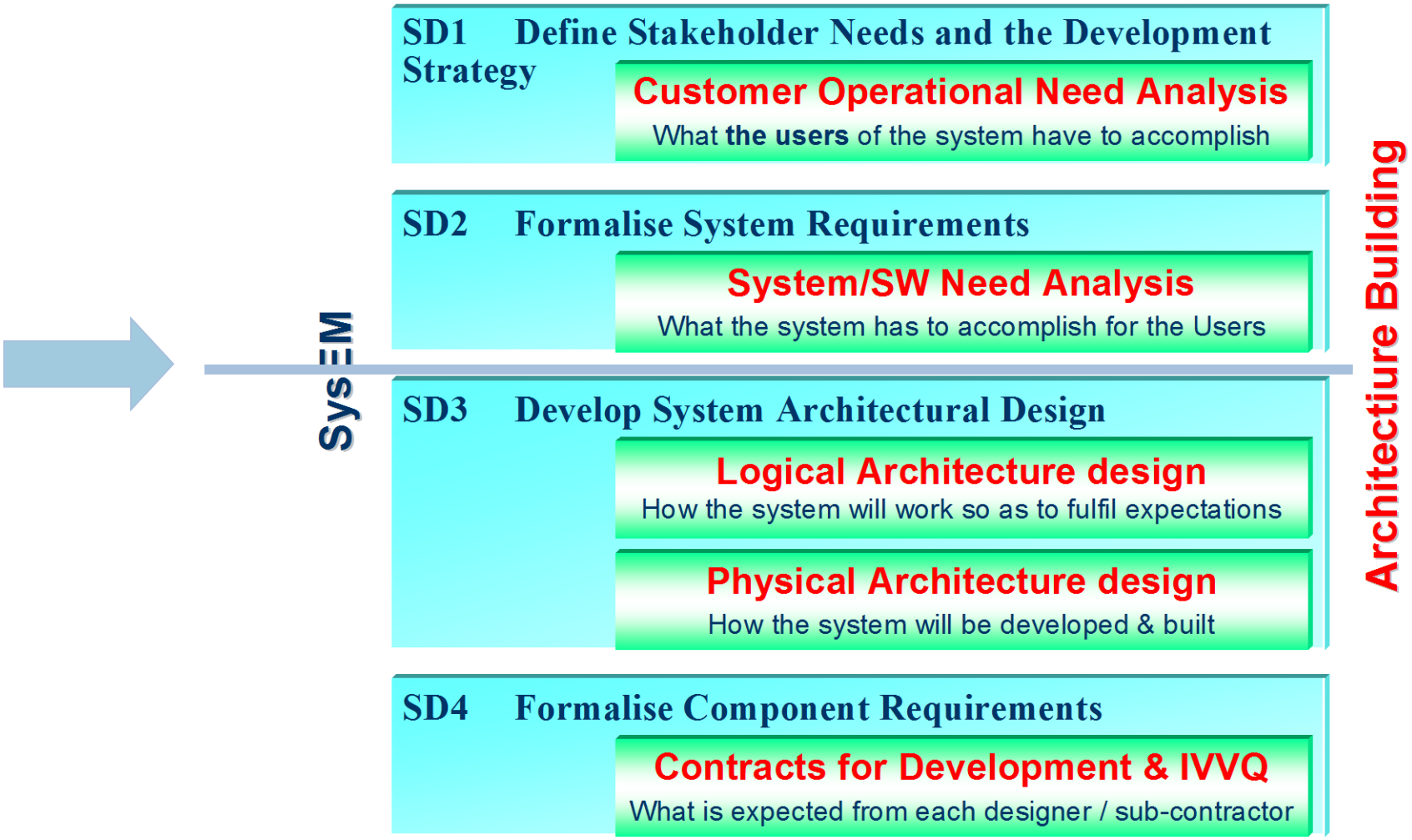
Develop integrated architecture to satisfy customer benchmarks

THALES

AIRBUS GROUP

SAFRAN

Architecture Development Process (2/2)



Agenda

- Avionics suite general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ candidate logical architectures
- Architecture building examples
  - Display primary parameters

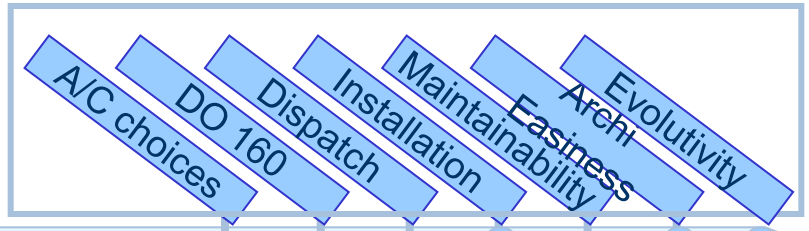
Architecture Main Drivers

- Operational drivers
  - Cockpit philosophy
  - Capacity requirements (CAT III, LPV, RNP-AR, VNAV …)
  - Maintainability and Dispatch requirements
- Functional drivers
  - CPU throughput sizing, I/O sizing, Safety requirements, latency
  - Memory (type, sizing, access needs, Power-off context saving)
- Non functional drivers
  - Environmental, Safety Airworthiness,…
- Platform drivers
  - Redundancy (availability) & integrity management
  - Required spare for growth margin / Upgradeability / Options
- Installation / Aircraft integration drivers
- Program drivers
  - NRC / RC objectives
  - Re-use / Product policy / Industrial share drivers
  - Development time

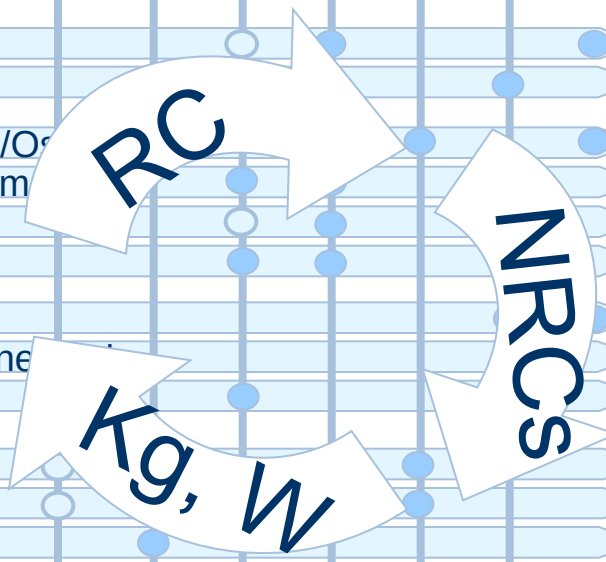
General non functional requirements

Physical Architecture Trade-off Items

- ☑ Data CPU throughput OK
- ☑ Graphics CPU throughput OK
- ☑ I/O Capacity OK
- ☑ Data flow Bus Capacity OK
- ☑ Latency constraints OK

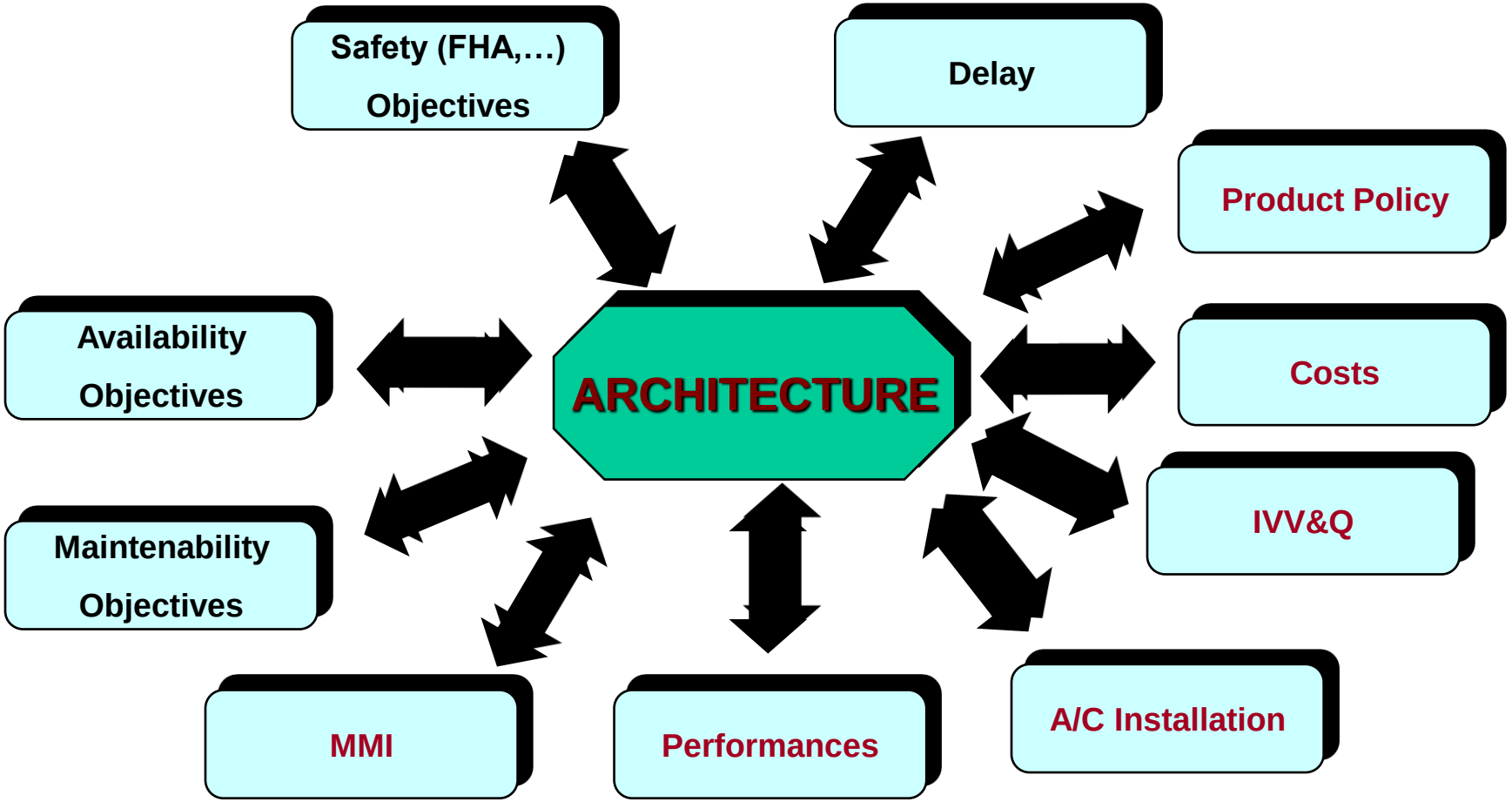


Computing Resources	Trade-Off
	Ex: Processing in Remote Controllers
Graphical Resources	DU Smart ←→ DU Dumb
	Ex: Displays network connectivity
I/O Resources	Distributed I/Os Mgt ←→ Centralized I/Os
	Dual I/O boards with wiring Y's ←→ Sim
	Others Trade-Off
	Others Trade-Off
Networks	High integrity network
	High Perf. N/W ←→ Low cost access ne
	Increased Network Redundancy
General IMA Architecture	Cabinet ←→ Stand-alones Racks
	Tray or racks ←→ Direct mounting
	Packaging Robustness
	Centralized PWR supplies ←→ Distributed
	Single bus bar or dual bus bars equipment
	Aircraft Power supply Specific Characteristics



Architecture = une synthèse complexe

GEA Tianjin / 中国民航大学中欧航空工程师学院

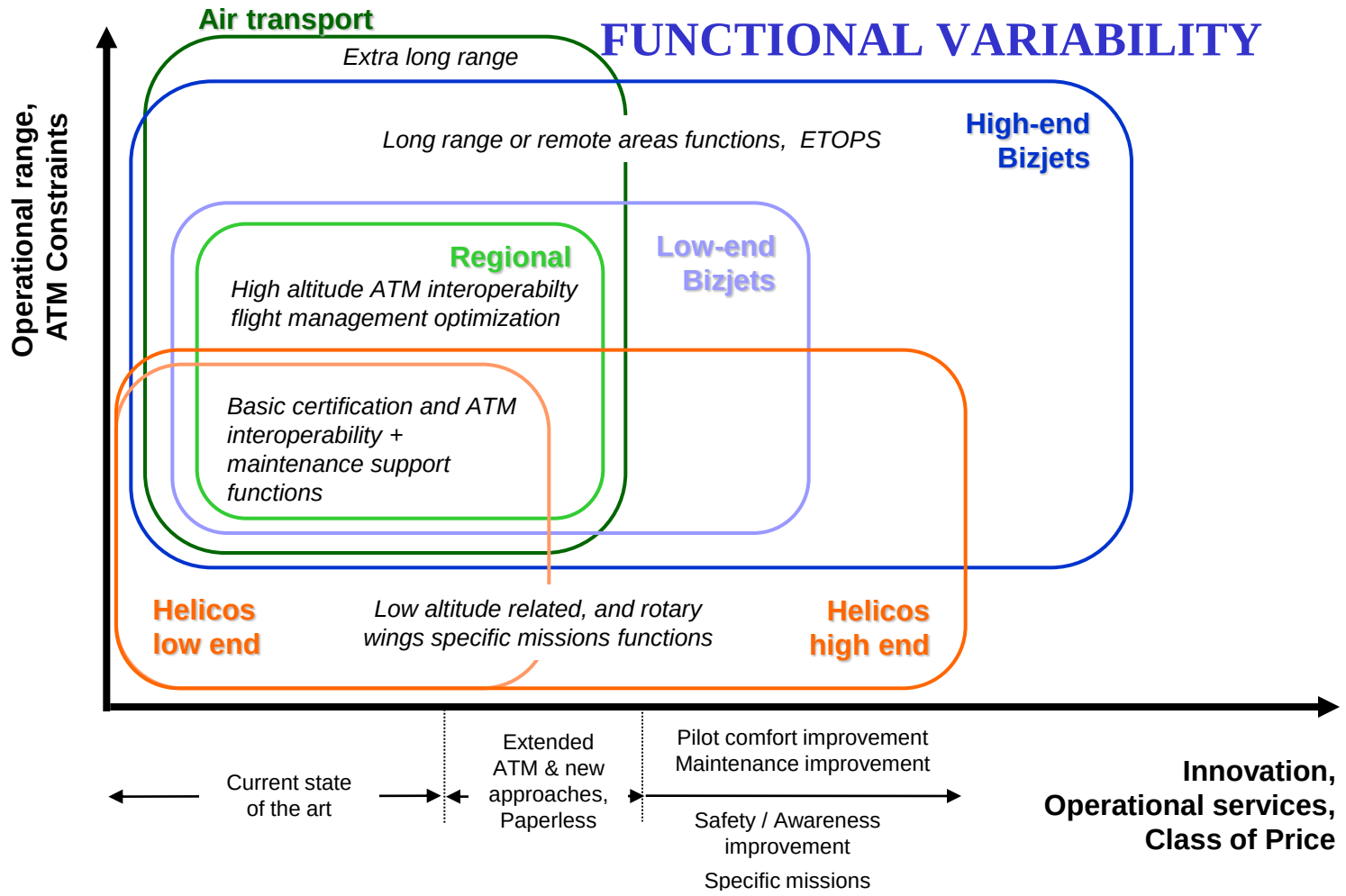


Architecture: A matter of "Trade Off" Art

Agenda

- Avionics suite general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ candidate logical architectures
- Architecture building examples
  - Display primary parameters

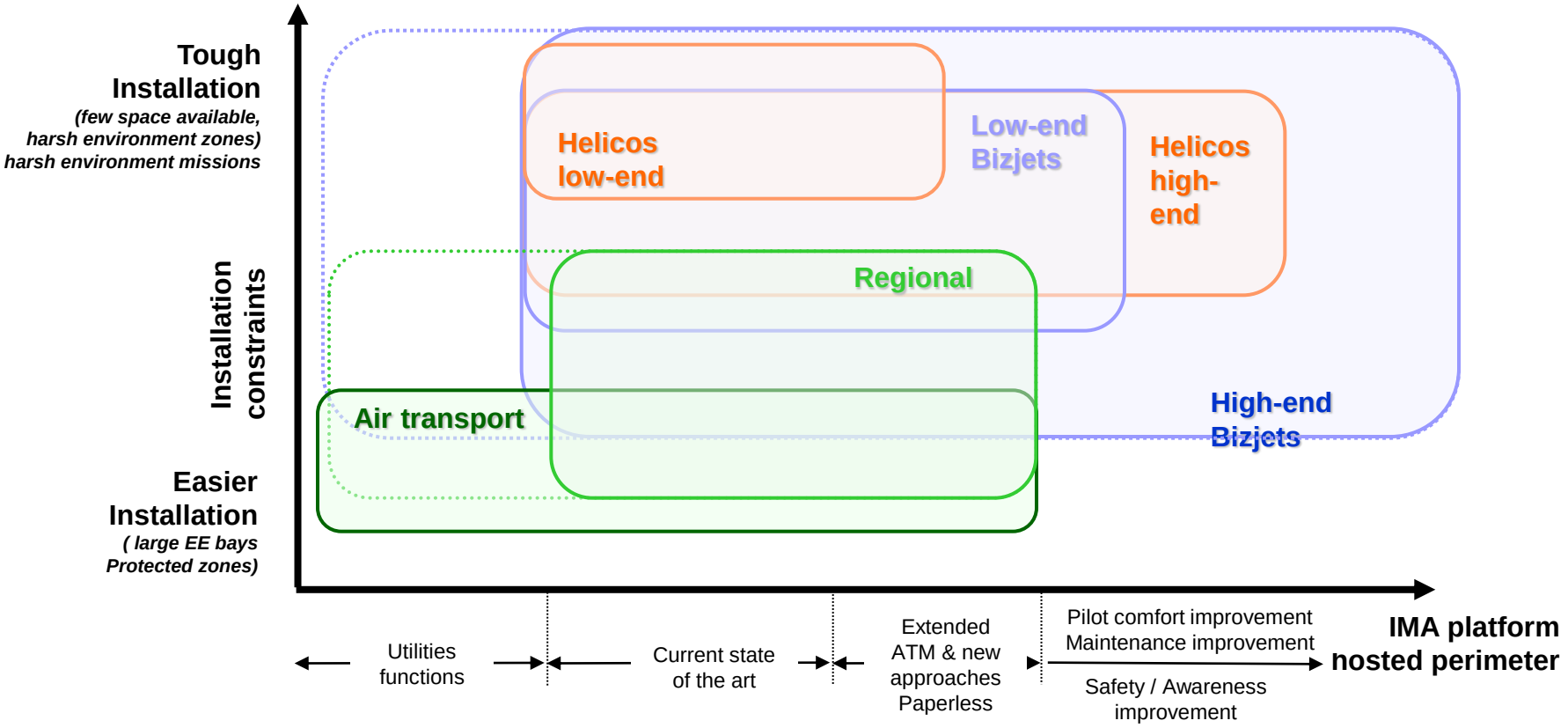
GEA Tianjin / 中国民航大学中欧航空工程师学院



Modular approach for the functional building blocks

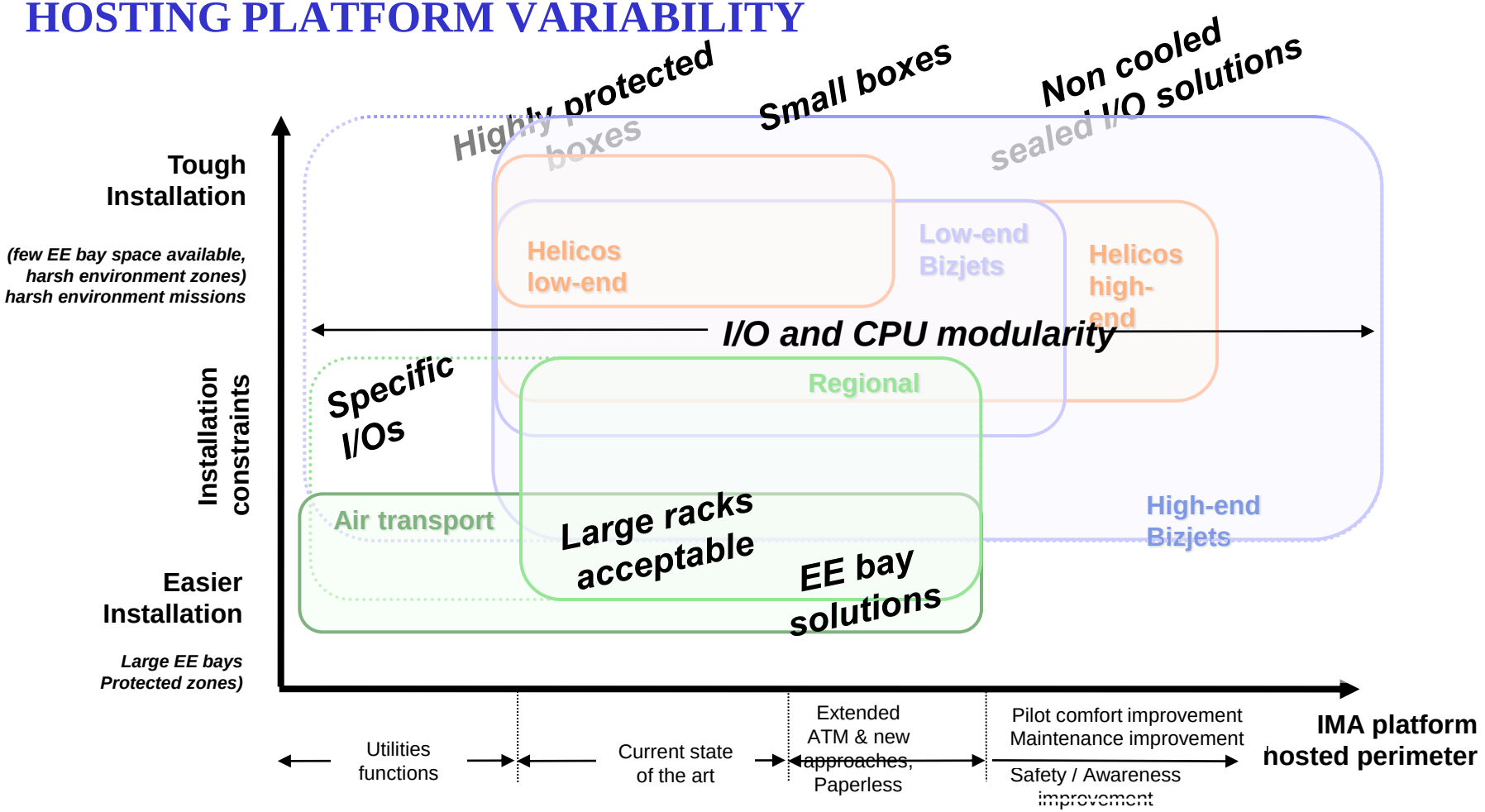
GEA Tianjin / 中国民航大学中欧航空工程师学院

HOSTING PLATFORM VARIABILITY



Significant Variability on Install Concerns

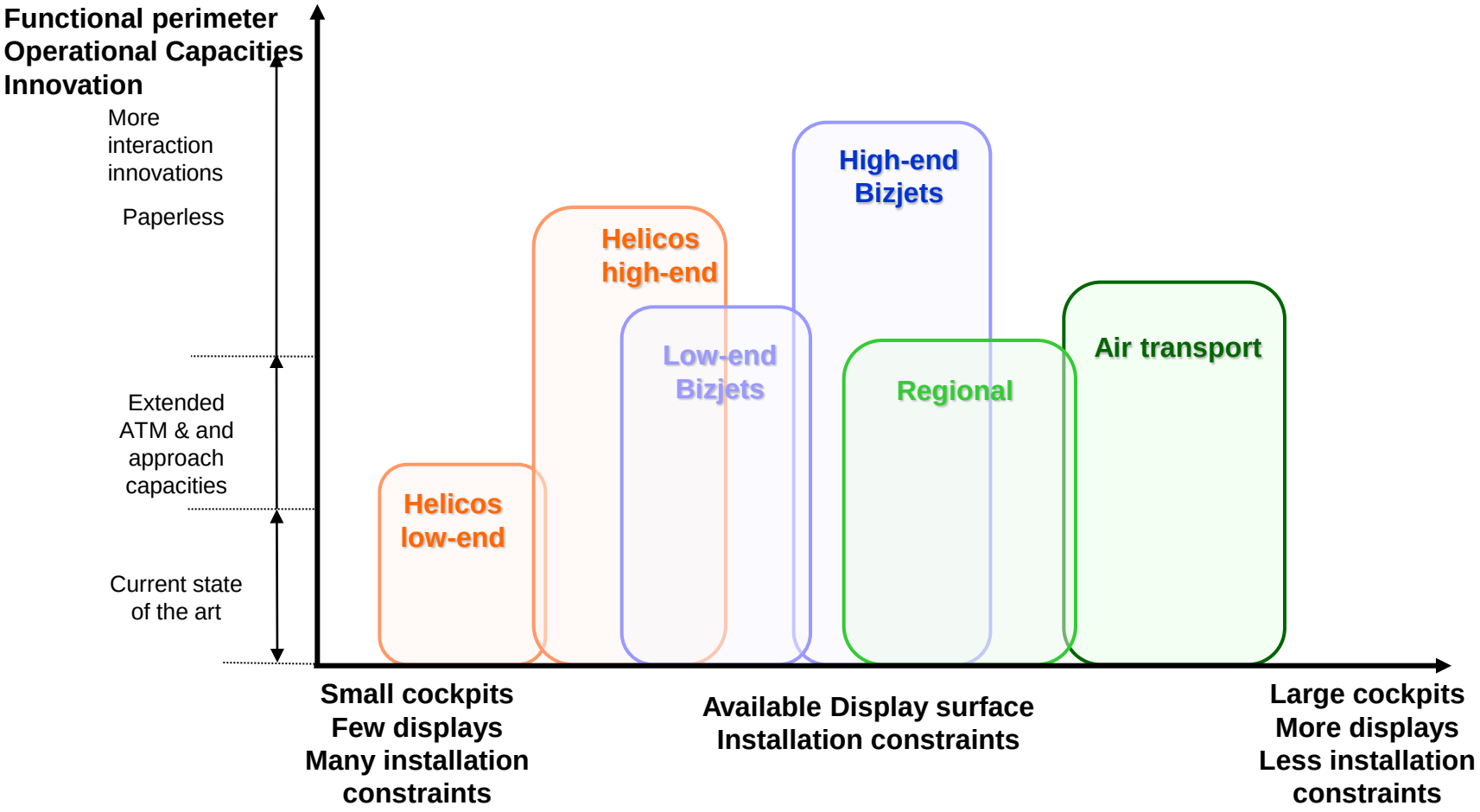
HOSTING PLATFORM VARIABILITY



Variability upon Plateforms form factor

GEA Tianjin / 中国民航大学中欧航空工程师学院

COCKPIT ELEMENTS VARIABILITY



A need to define Modular Cockpit Solutions

Agenda

- Avionics suite general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ candidate logical architectures
- Architecture building examples
  - Display primary parameters

Architecture Building Rule-of-Thumb

- Functions Availability Concerns
  - *Loss of all attitude displays including standby: Catastrophic*
- Functions Integrity Concerns
  - *Display of misleading attitude information on both primary displays : Catastrophic*

Architecture Building Rule-of-Thumb

Functions Availability Considerations

Some functions are absolutely necessary for a "**Continuous Safe Flight and Landing**" whatever systems malfunction is subject to occur in the aircraft

- Loss of these functions is considered as a **catastrophic** event
- Rule of design consists in providing at least a **3 or 4-channels redundancy (*)**
- Additional **dissimilarity** design rules do apply (single event [e.g. design flaw] can not lead to a catastrophic situation)
- 3 or 4-level redundancy depends on the specific system components MTBF, flight duration and dispatch reliability considerations (ability to take-off with one failure)

Catastrophic Functions
➔ 3 or 4 channels
➔ Dissimilarity required

(*) One channel can be composed of one or several computing lanes
It depends on integrity requirements and hardware safety characteristics

Architecture Building Rule-of-Thumb

– Functions Availability Considerations (Cont'd)

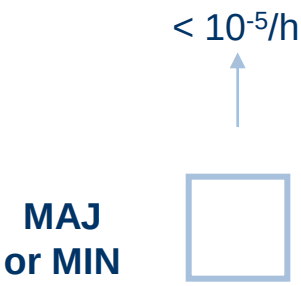
Loss of other functions lead to operational situations which are evaluated as Hazardous, Major or Minor situations

- Besides CSFL functions, avionics functions are most generally **essential** (effect of their loss is Major), or **non-essential** (Minor)
- **Essential** functions
  - » Rule of design consists in providing a **2 or 3-channels redundancy**
  - » 2 or 3 redundancy depends mostly on dispatch reliability considerations (ability to take-off with one failure) – No general rule
- **Non-Essential** functions
  - » Rule of design consists in providing a **1-channel redundancy**
  - » Minor criticality means that the effect of the loss of such functions has no significant impact on the flight, hence dispatch of the aircraft without this function is acceptable (with operational limitations)
  - » A 2-channel redundancy is sometimes provided upon economic considerations to avoid potential operational limitations (e.g. weather radar)

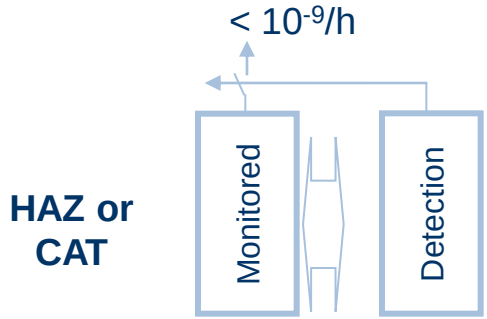
Essential (Major) ➔ 2 or 3 channels
Non-essential (Minor) ➔ 1 or 2 channels

Architecture Building Rule-of-Thumb

- **Functions Integrity Considerations**
  - Integrity requirements address the effect of potential undetected malfunctions (erroneous data computation, erroneous control, ..)
  - Integrity requirements are derived by the introduction of safety monitoring features which aims at improving the detection of malfunctions
    - A single thread computation channel has generally the following intrinsic failure detection capability
      10^{-7}/h < Undetected erroneous computation < 10^{-5}/h
    - **Rule-of-Thumb**: Any function whose integrity requirement is worse than major will have to be monitored against another channel



Single thread computation intrinsic failure detection capability



If detection and passivation mechanisms are independent from monitored channel

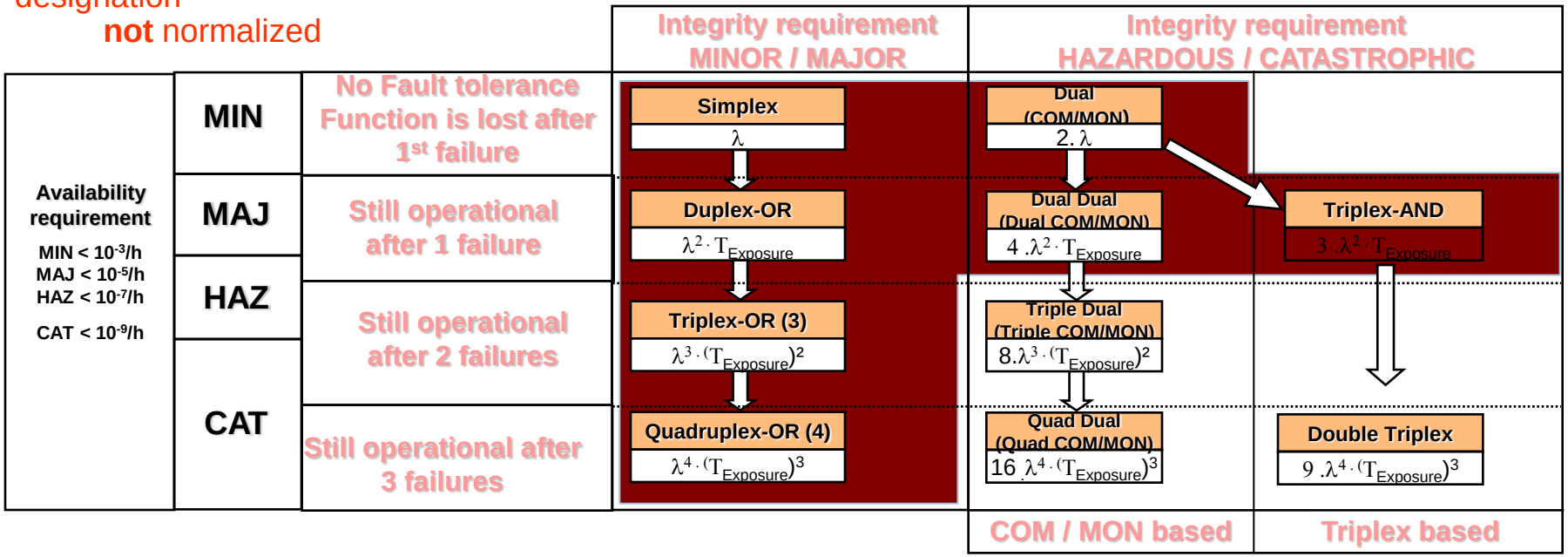
Agenda

- Avionics suite general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
  - Generational improvements
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ candidate logical architectures
- Architecture building examples
  - Display primary parameters

GEA Tianjin / 中国民航大学中欧航空工程师学院

Safety Requirements ⟷ Candidate Architectures

⚠ Architectures designation **not** normalized



Suite

- For illustration purpose only: not meant to be exhaustive, neither valid in all cases – Dissimilarity aspects not addressed

☛ Click on Architecture name to visualize architecture

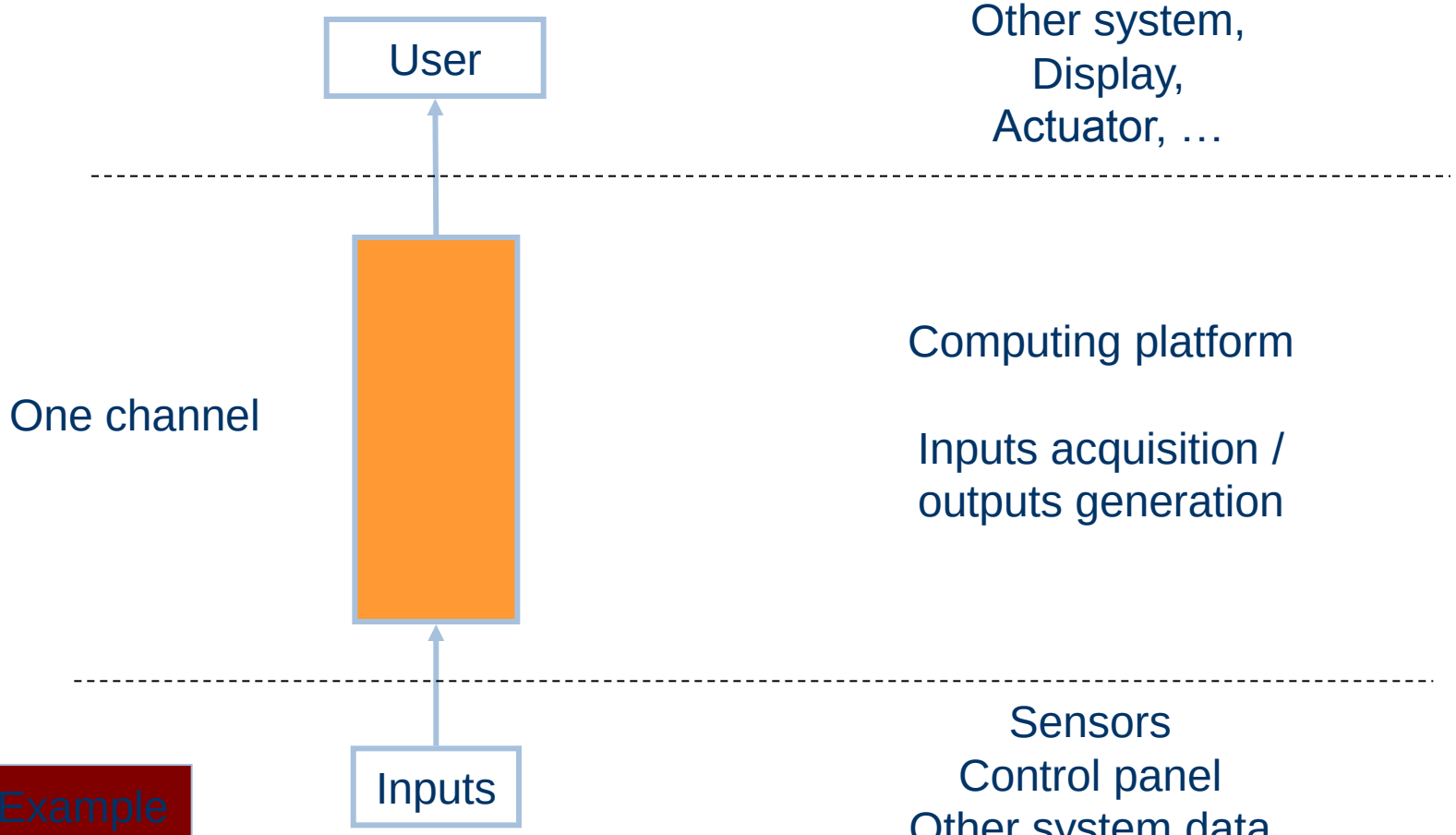
- Assumption on computing platform
  - Integrity: 10^{-7}/h < Undetected erroneous computation < 10^{-5}/h
  - Availability: 10^{-5}/h < λ < 10^{-3}/h

GEA Tianjin / 中国民航大学中欧航空工程师学院

Simplex Architecture

Availability capability: MIN
Integrity capability : MAJ

10^{-5}/h < Loss of function < 10^{-3}/h
10^{-7}/h < Erroneous control < 10^{-5}/h

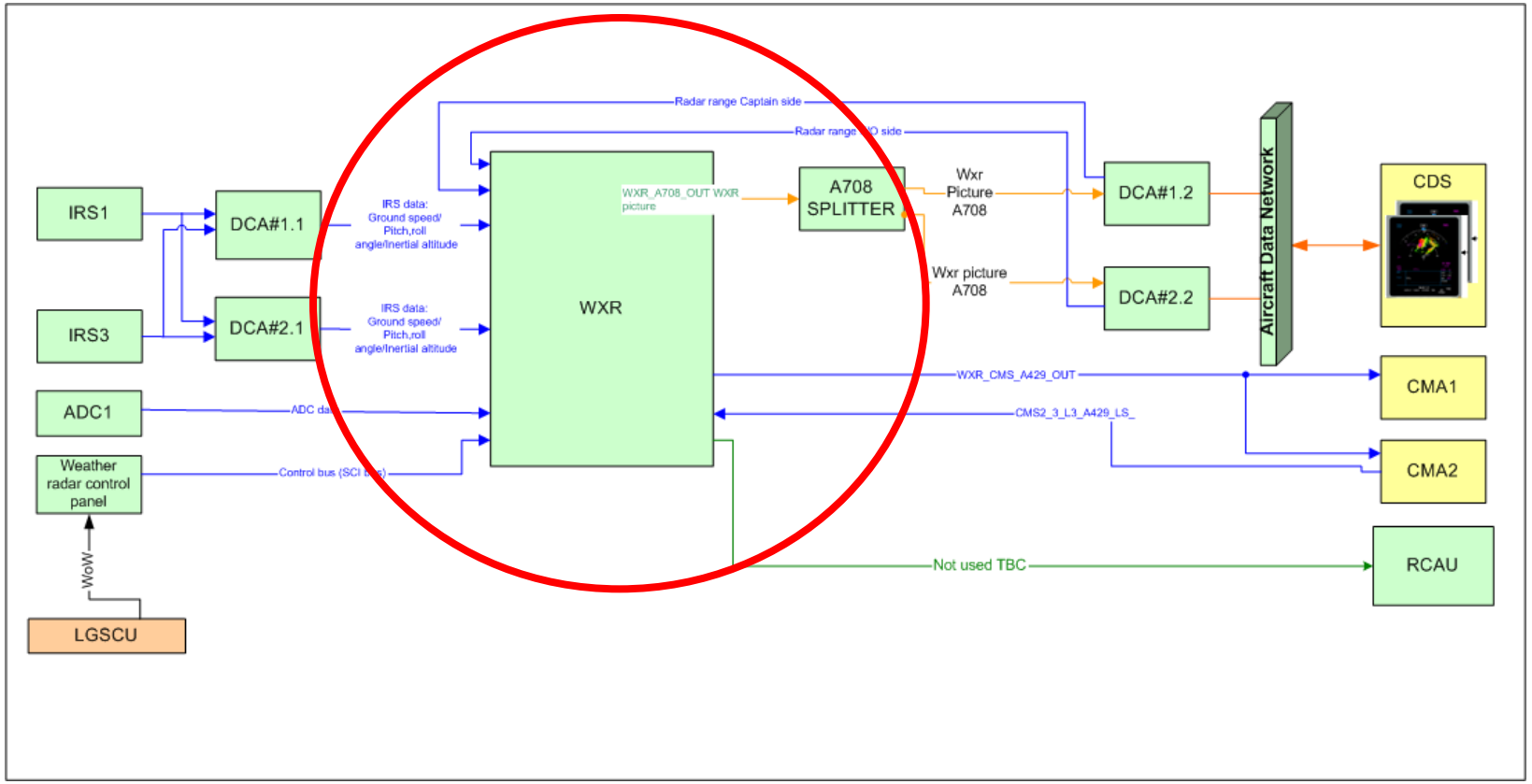


Click anywhere to come back to summary table

GEA Tianjin / 中国民航大学中欧航空工程师学院

Simplex Architecture

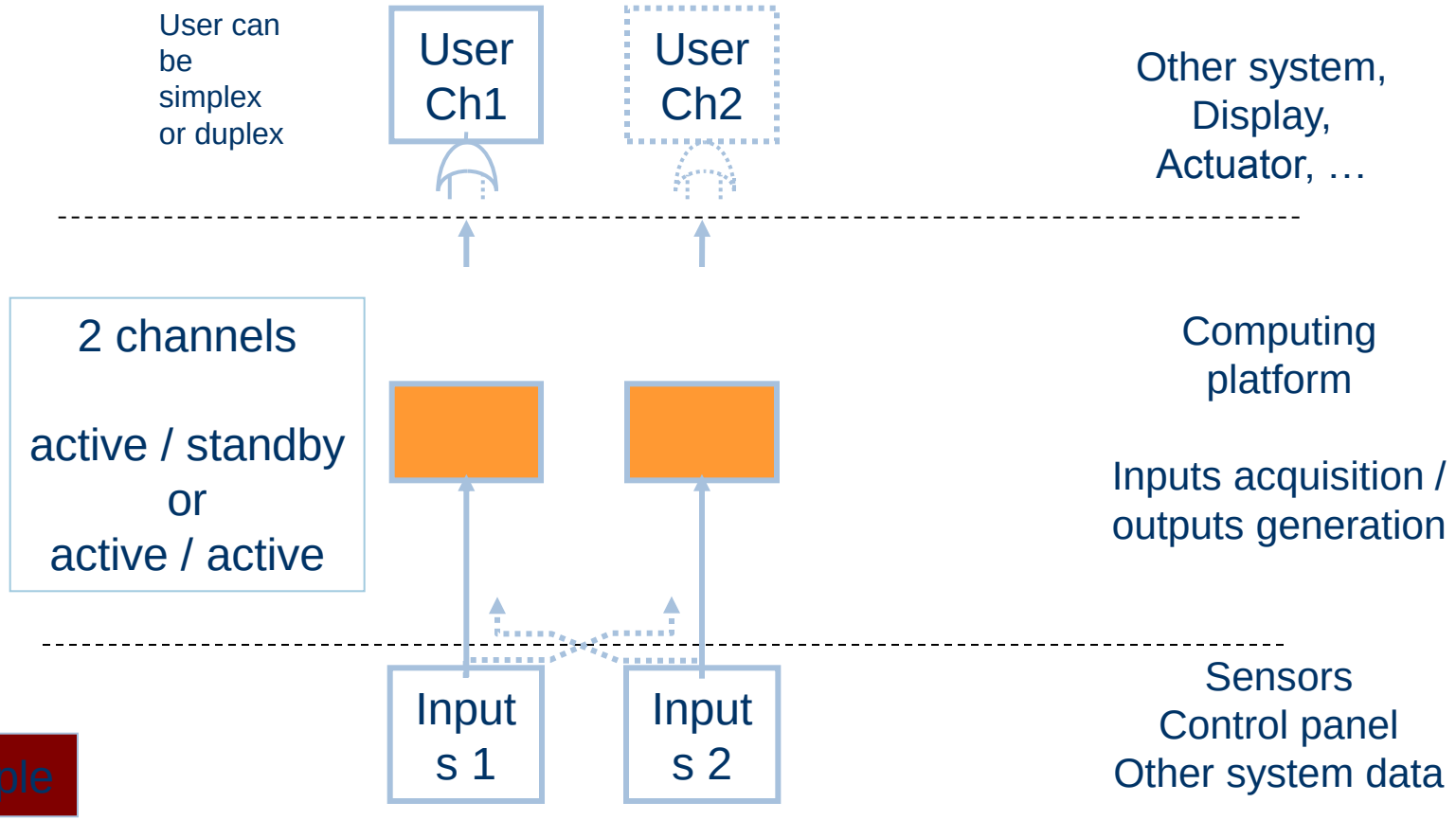
Weather Radar



Duplex Architecture

Availability capability: MAJ - HAZ
Integrity capability: MAJ

10^{-7}/h - 10^{-9}/h < Loss of function < 10^{-5}/h - 10^{-7}/h
10^{-7}/h < Erroneous cntrl < 10^{-5}/h

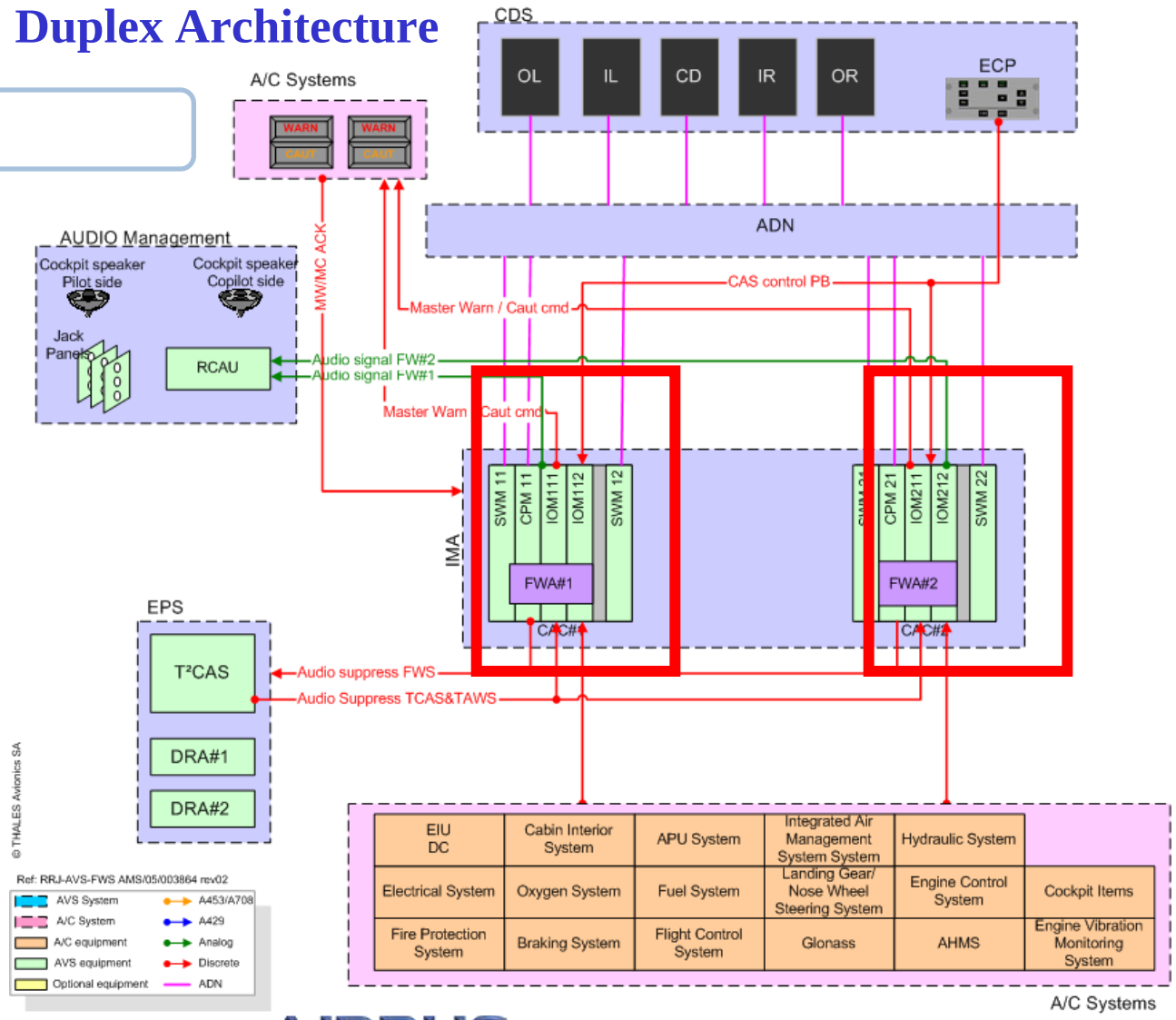


Example

GEA Tianjin / 中国民航大学中欧航空工程师学院

Duplex Architecture

Flight Warning



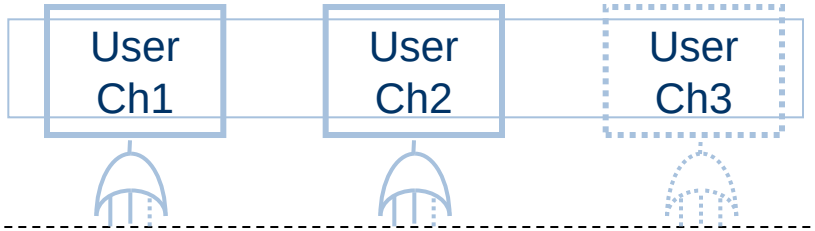
Click anywhere to come back to summary table

GEA Tianjin / 中国民航大学中欧航空工程师学院

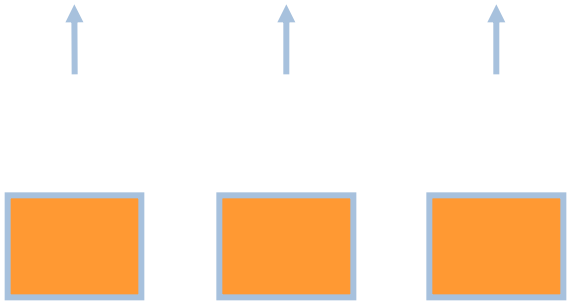
Triplex-ORed Architecture

Availability capability: HAZ - CAT
Integrity capability: MAJ

Loss of function < 10^{-7}/h - 10^{-9}/h
10^{-7}/h < Erroneous cntrl < 10^{-5}/h



Other system,
Display,
Actuator, …

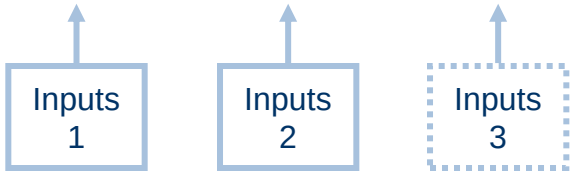


3 channels

active / active / active
or
active / standby / standby
or
active / active / standby

Computing platform

Inputs acquisition /
outputs generation



Example

Sensors
Control panel
Other system data

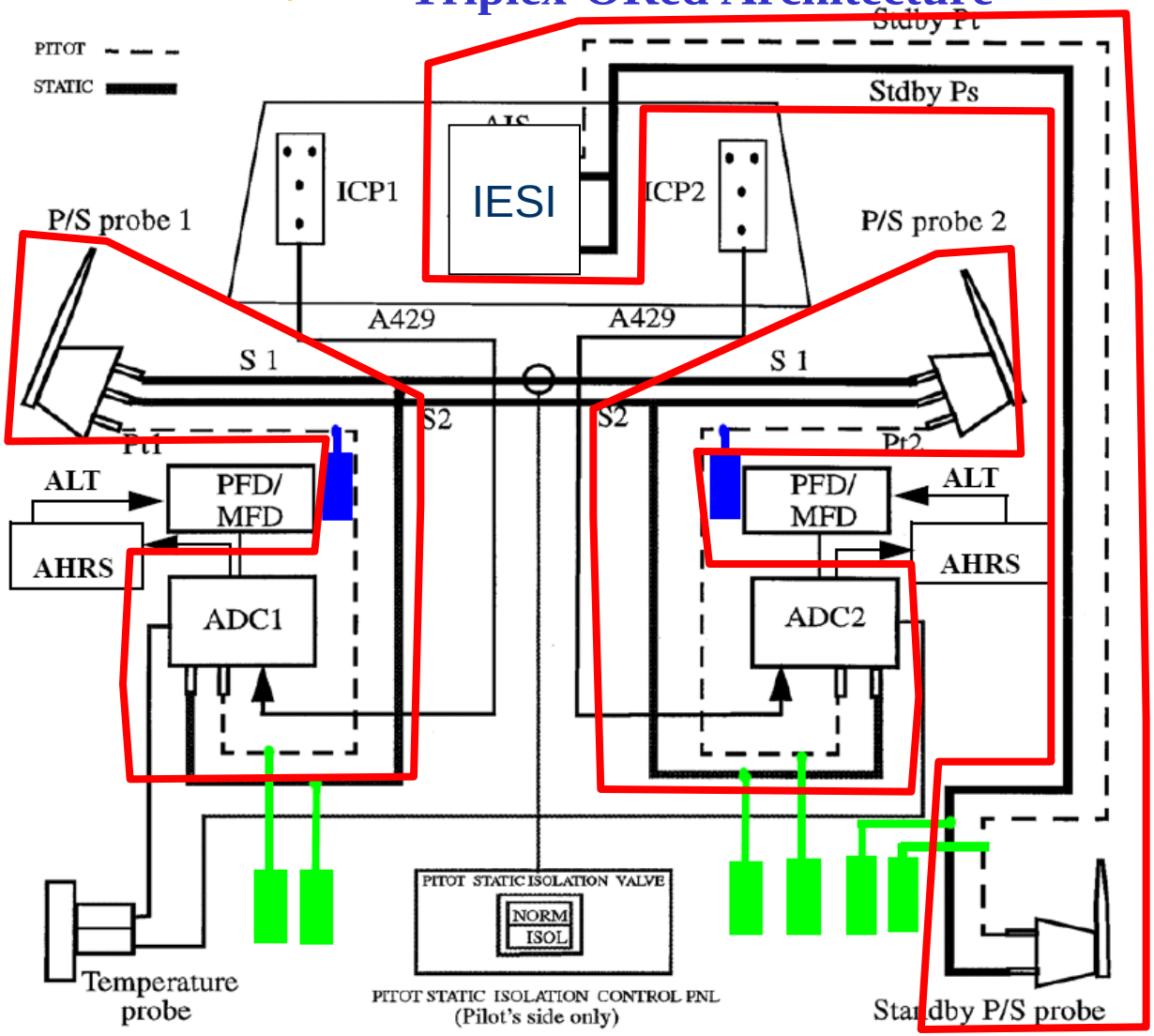
THALES

AIRBUS GROUP

SAFRAN

Click anywhere to come back to summary table

Triplex-ORed Architecture



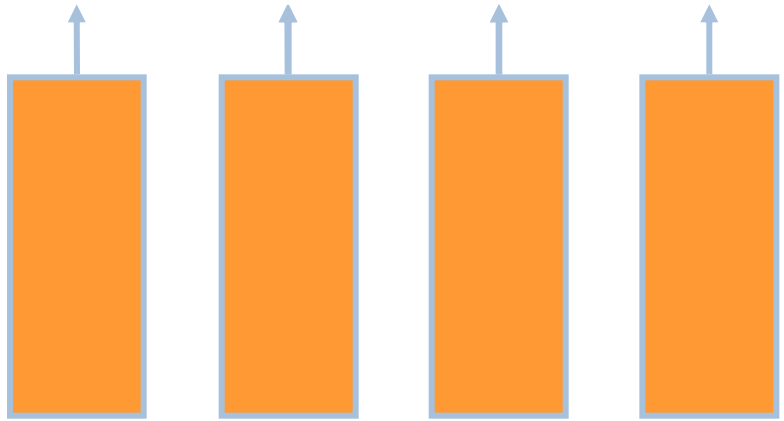
GEA Tianjin / 中国民航大学中欧航空工程师学院

Quadruplex-ORed Architecture

Availability capability: CAT
Integrity capability: MAJ

Loss of function < 10^{-9}/h
10^{-7}/h < Erroneous cntrl < 10^{-5}/h

Other system, Display, Actuator, …



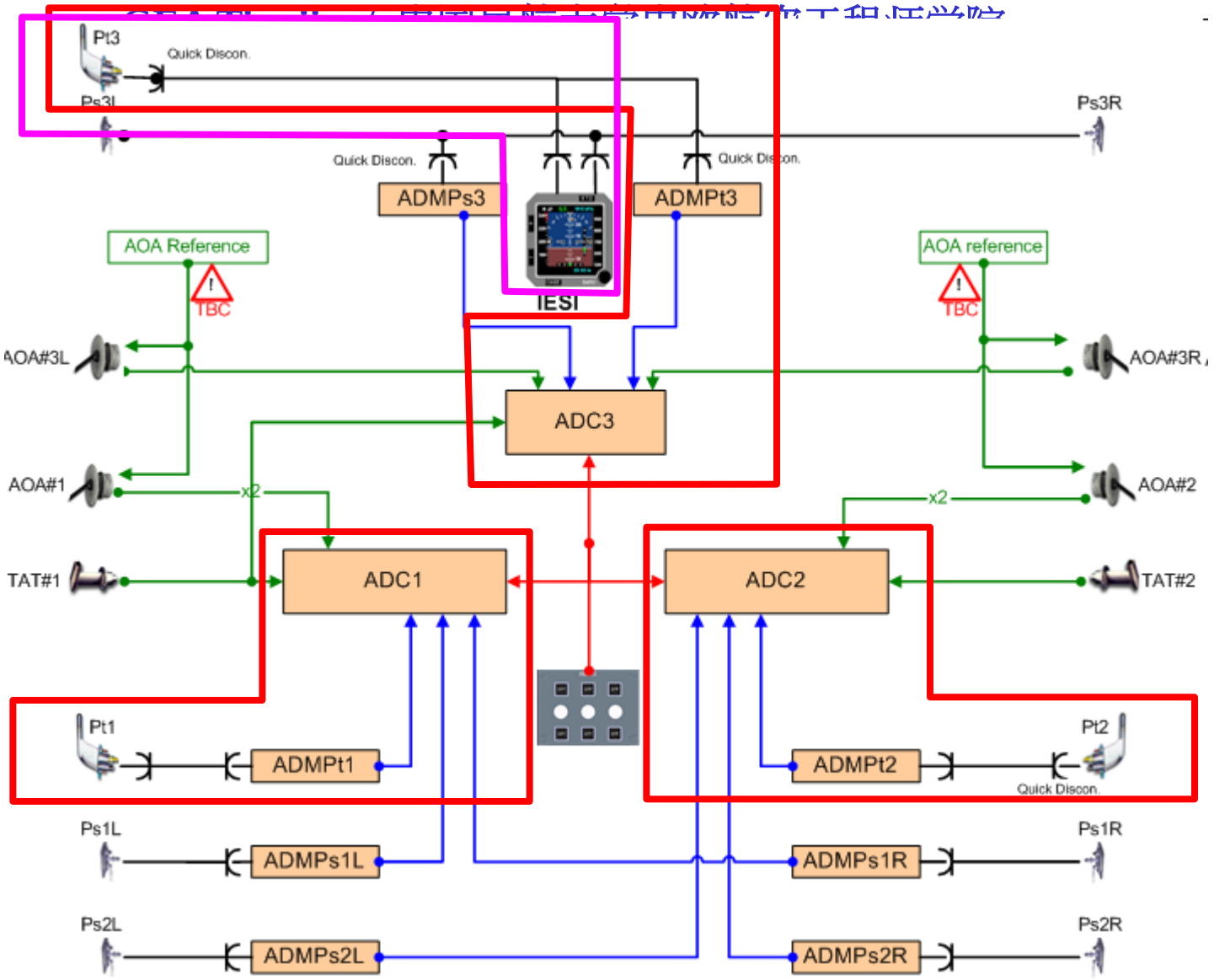
Computing platform

Inputs acquisition / outputs generation

Example

Sensors
Control panel
Other system data

THALES AIRBUS GROUP SAFRAN


Pt3
Quick Discon.
Ps3L
Ps3R
Quick Discon.
Quick Discon.
ADMPs3
ADMPt3
AOA Reference
TBC
IESI
AOA reference
TBC
AOA#3L
AOA#3R
ADC3
AOA#1
x2
x2
AOA#2
TAT#1
ADC1
ADC2
TAT#2
Pt1
ADMPt1
ADMPt2
Pt2
Quick Discon.
Ps1L
ADMPs1L
ADMPs1R
Ps1R
Ps2L
ADMPs2L
ADMPs2R
Ps2R

Click anywhere to come back to summary table

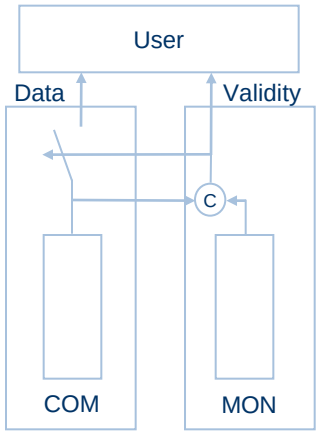
GEA Tianjin / 中国民航大学中欧航空工程师学院

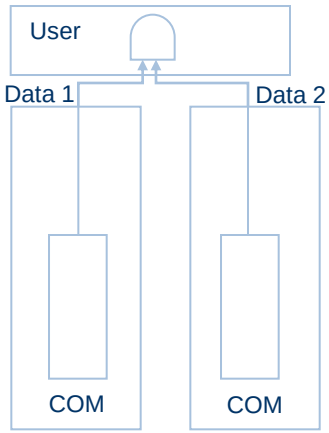
Availability capability: MIN
Integrity capability: CAT

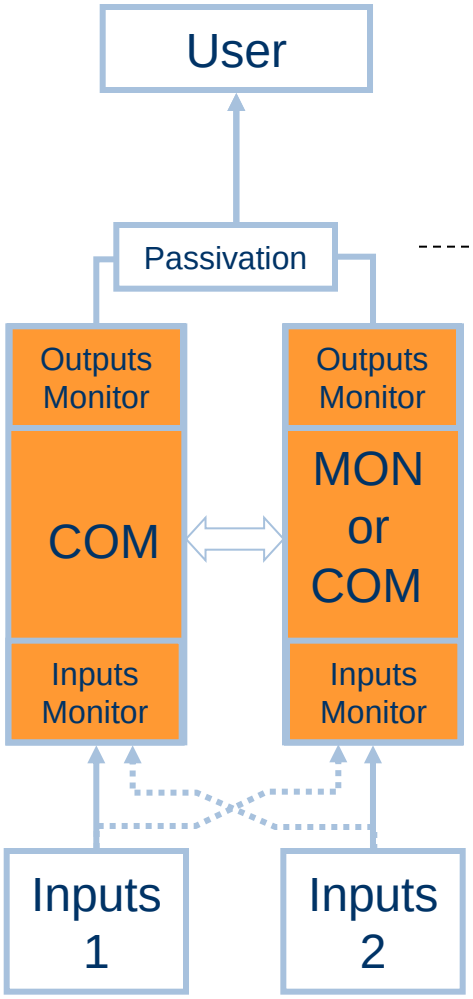
Dual or COM/MON

10^{-5}/h < Loss of one channel < 10^{-3}/h
Erroneous cntrl < 10^{-9}/h

Passivation mechanism or logic located in User system or in COM/MON







Other system, Display, Actuator, …

Computing platform

Inputs acquisition / outputs generation

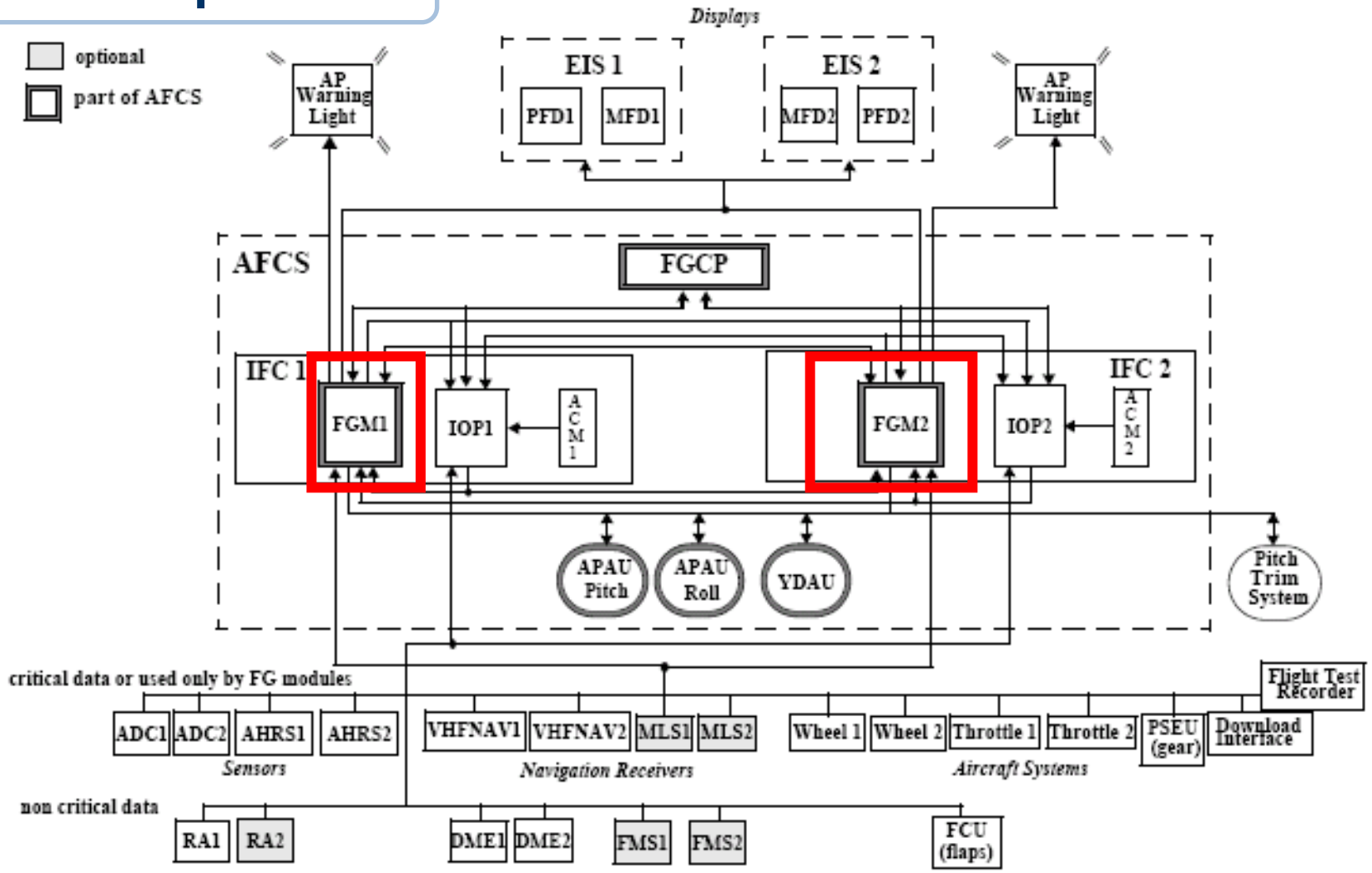
Sensors
Control panel
Other system data

Example

THALES AIRBUS GROUP SAFRAN

Autopilot

Dual or COM/MON



GEA Tianjin / 中国民航大学中欧航空工程师学院

Dual Dual or Dual COM/MON

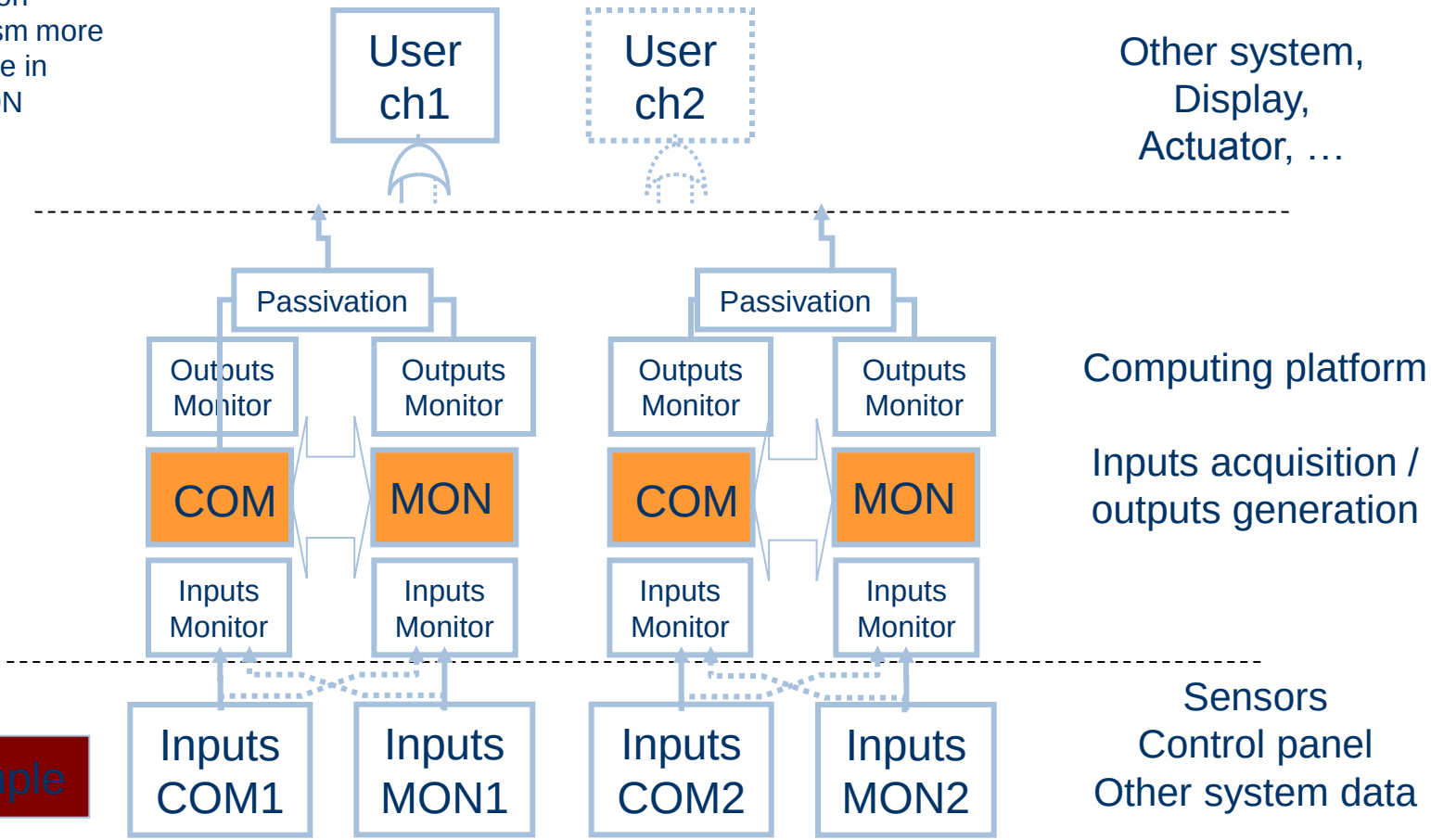
Availability capability: MAJ

Integrity capability: CAT

10^{-7}/h < Loss of function < 10^{-5}/h

Erroneous cntrl < 10^{-9}/h

Passivation mechanism more likely to be in COM/MON

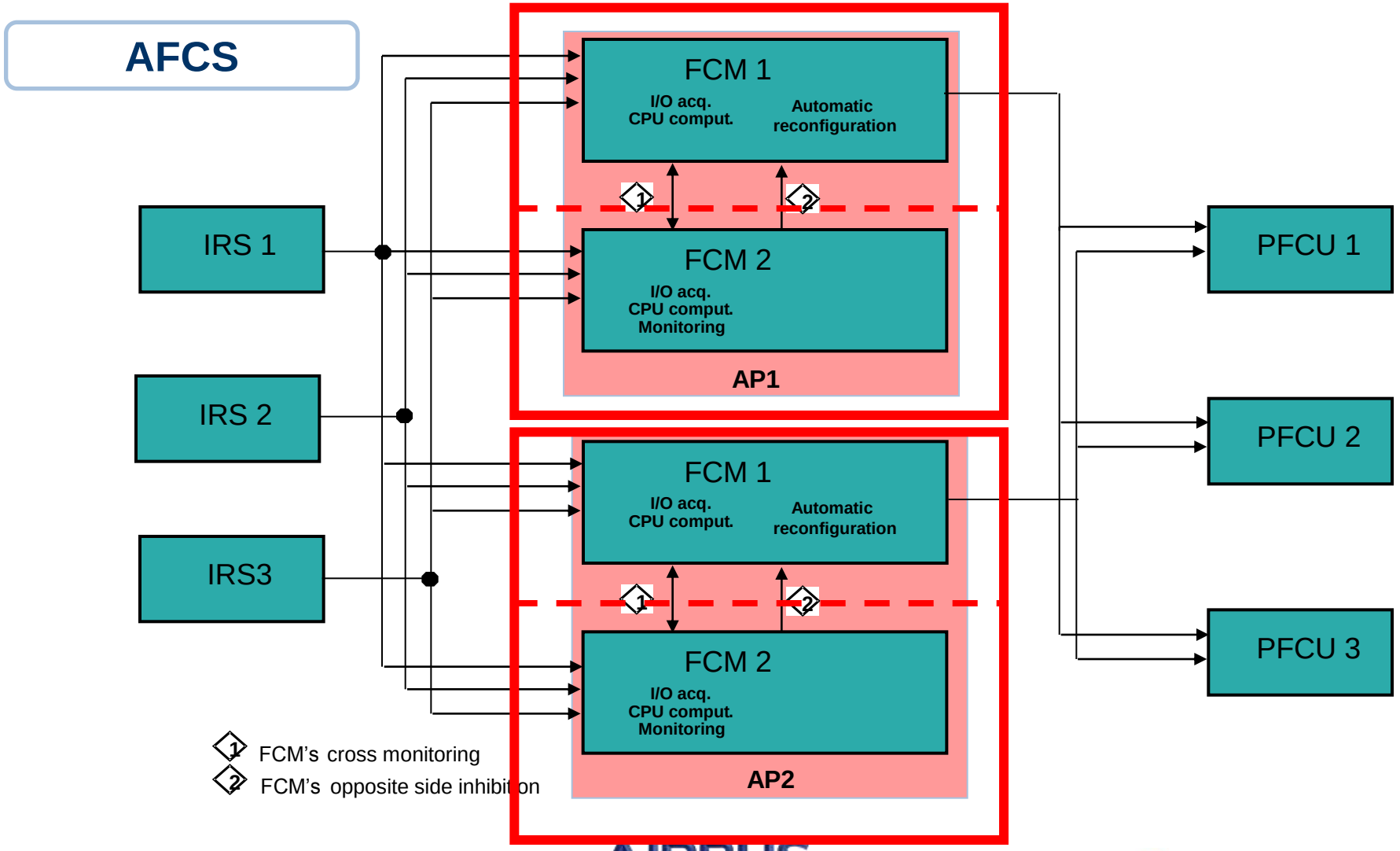


Example

THALES AIRBUS GROUP SAFRAN

GEA Tianjin / 中国民航大学中欧航空工程师学院

Dual Dual or Dual COM/MON



GEA Tianjin / 中国民航大学中欧航空工程师学院

Triple Dual Architecture

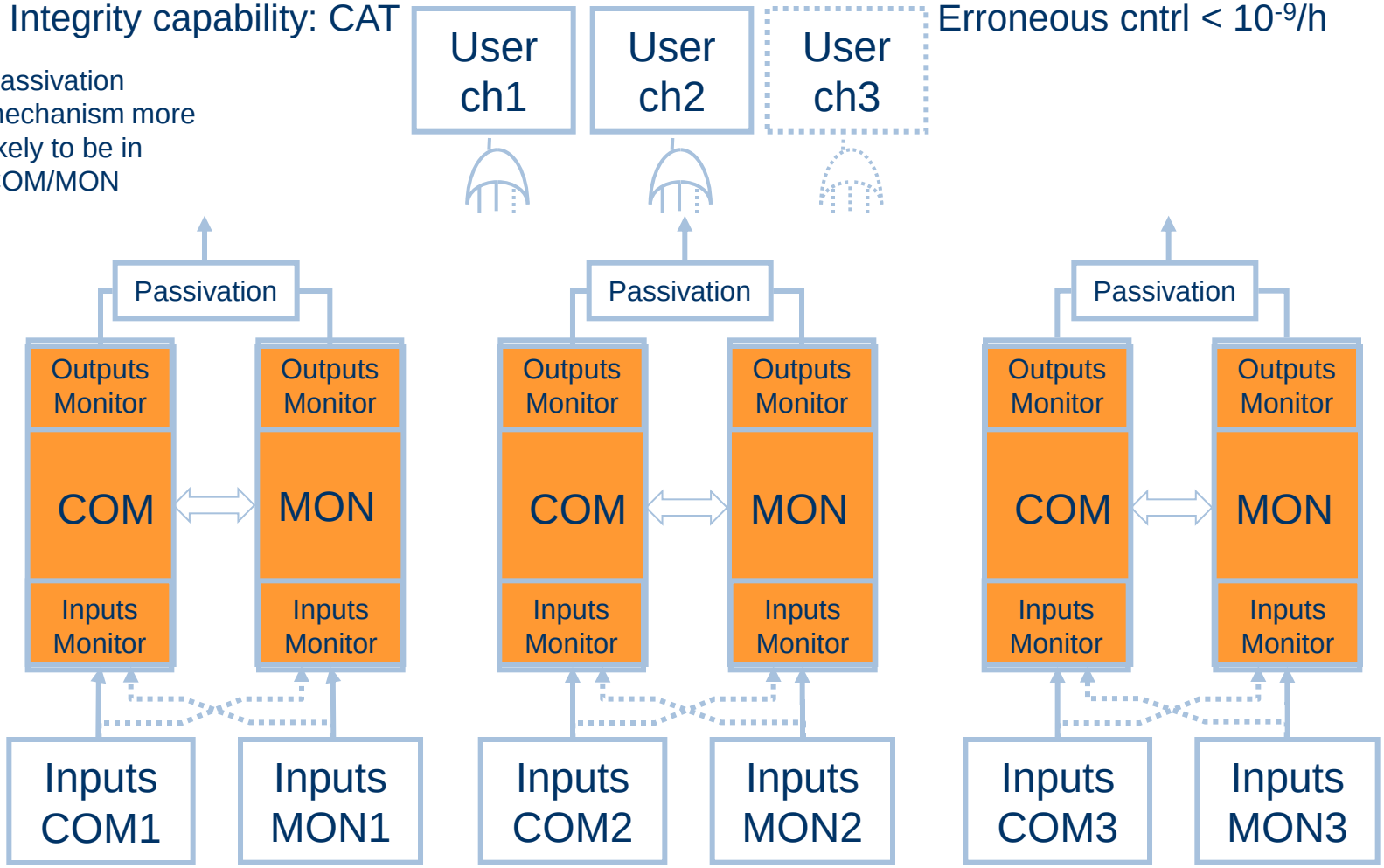
Availability capability: HAZ - CAT

Integrity capability: CAT

Loss of function < 10^{-7}/h - 10^{-9}/h

Erroneous cntrl < 10^{-9}/h

Passivation mechanism more likely to be in COM/MON



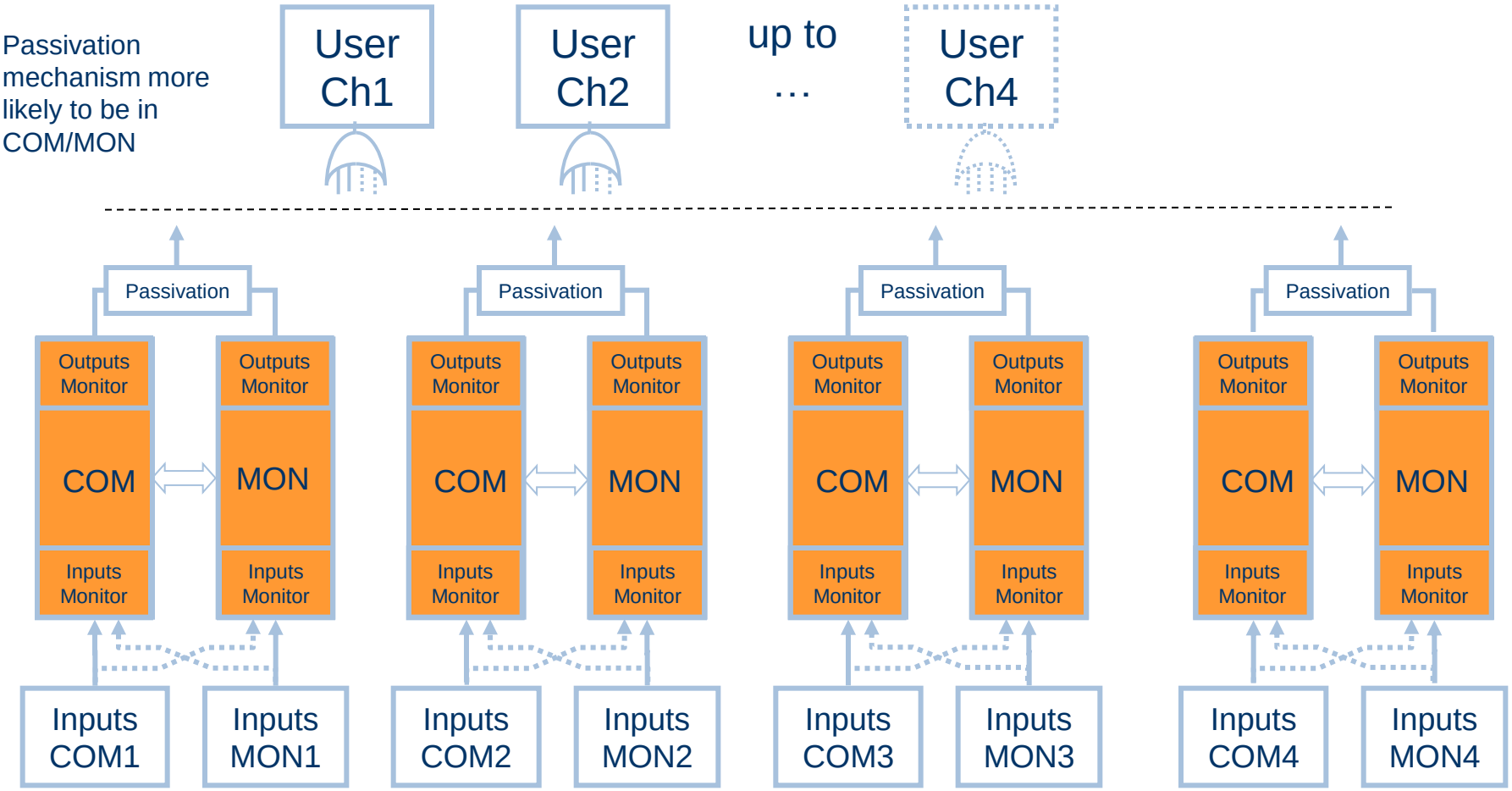
CEA Tianjin / 中国民航大学中欧航空工程师学院

Availability capability: CAT
Integrity capability: CAT

Quad Dual Architecture

Loss of function < 10^{-9}/h
Erroneous cntrl < 10^{-9}/h

Passivation mechanism more likely to be in COM/MON



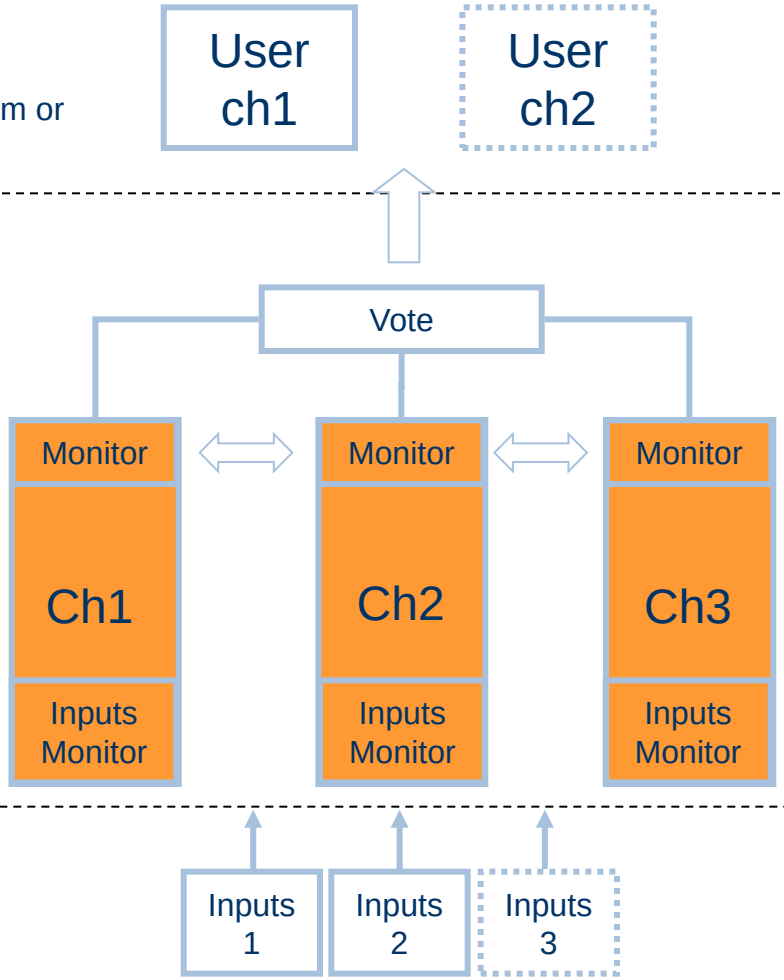
GEA Tianjin / 中国民航大学中欧航空工程师学院

Availability capability: MAJ/HAZ — 10^{-8}/h < Loss of function < 10^{-5}/h

Integrity capability: CAT — Erroneous cntrl < 10^{-9}/h

Triplex-AND Architecture

Vote passivation mechanism or logic located in User system or in triplex archi

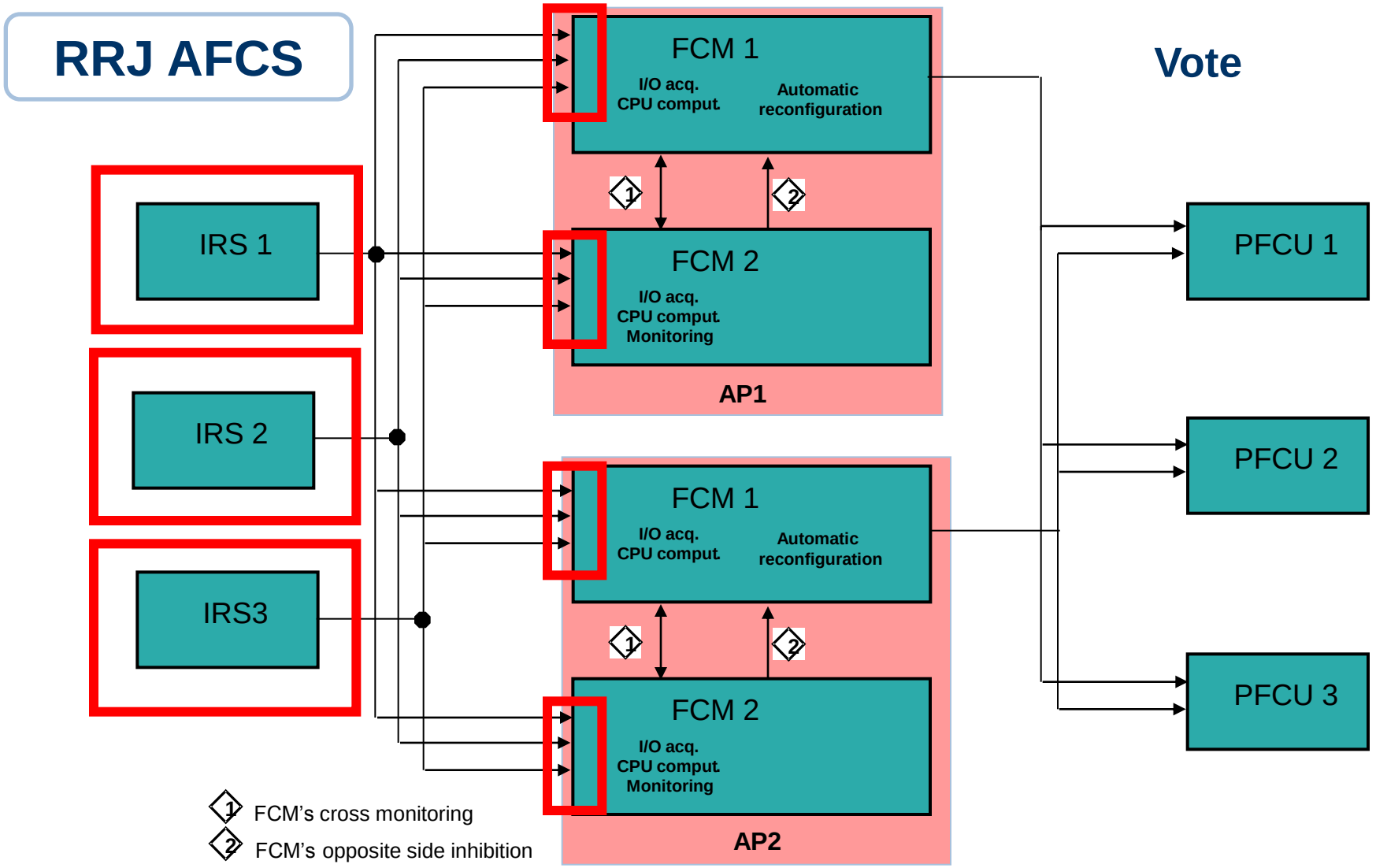


Example

Click anywhere to come back to summary table

Triplex-AND Architecture

GEA Tianjin / 中国民航大学中欧航空工程师学院



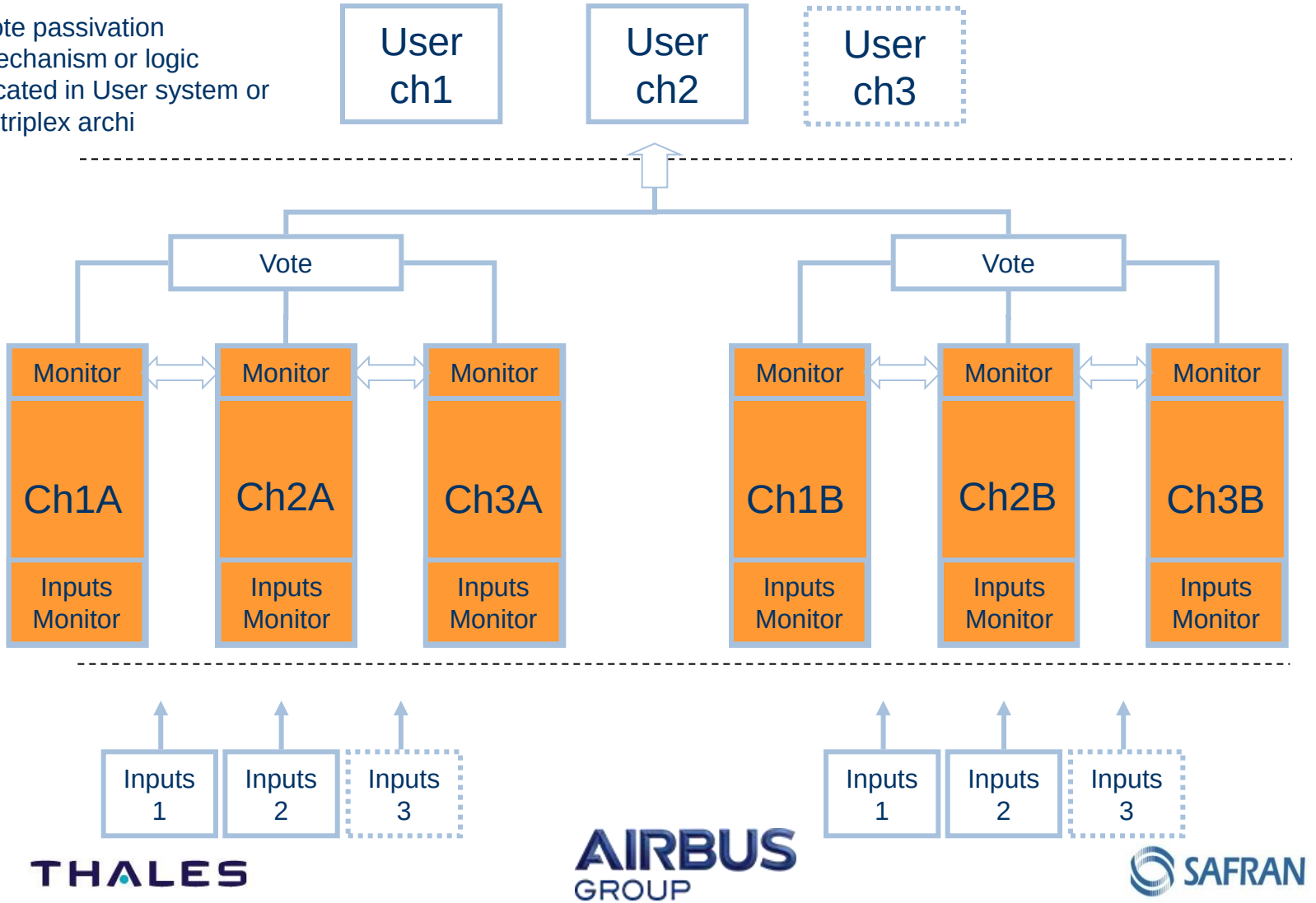
GEA Tianjin / 中国民航大学中欧航空工程师学院

Availability capability: CAT
Integrity capability: CAT

Loss of function < 10^{-9}/h
Erroneous cntrl < 10^{-9}/h

Double Triplex-AND Architecture

Vote passivation mechanism or logic located in User system or in triplex archi



Agenda

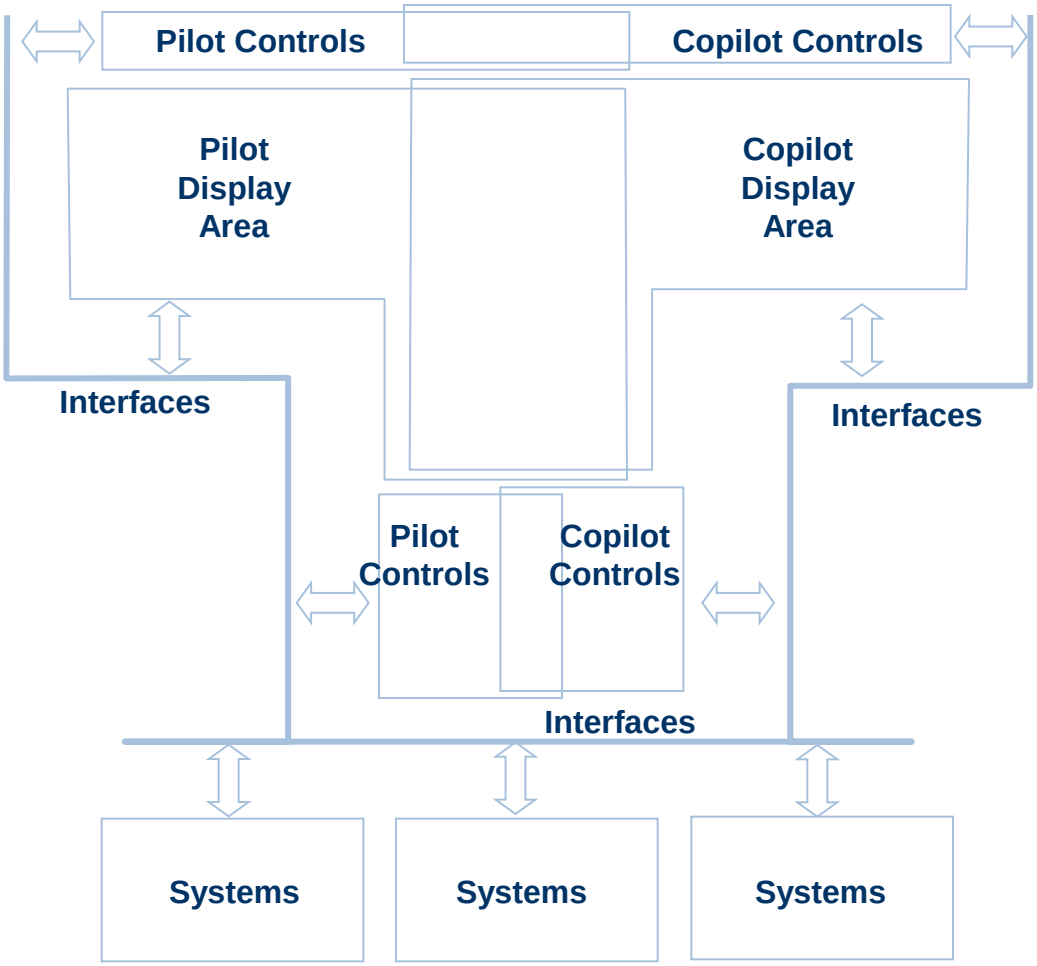
- Avionics suite general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
  - Generational improvements
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ candidate logical architectures
- Architecture building examples
  - Display primary parameters

Avionics Suite - General

- An Avionics Suite is composed of
  - A **Display System** that provides to the crew the necessary **visual** information (PFD, ND, EWD, SD, ...)
  - **Means of control** for the crew **to configure** the various systems. They can be either:
    - Dedicated to one specific operational activity (Radio Management Panel)
    - But, more and more shared by several systems (track-ball, keyboard)
  - **Peripheral systems** that provide **operational services** to the crew or to other systems
    - Using the Display system obviously as the main shared HMI mean
    - Potentially using IMA elements as a hosting platform for part or all of their component functions
    - With their own sensors, actuators or other specific peripherals
  - An **interface standard** as the main **communication media** between the various systems (A429, AFDX, …)

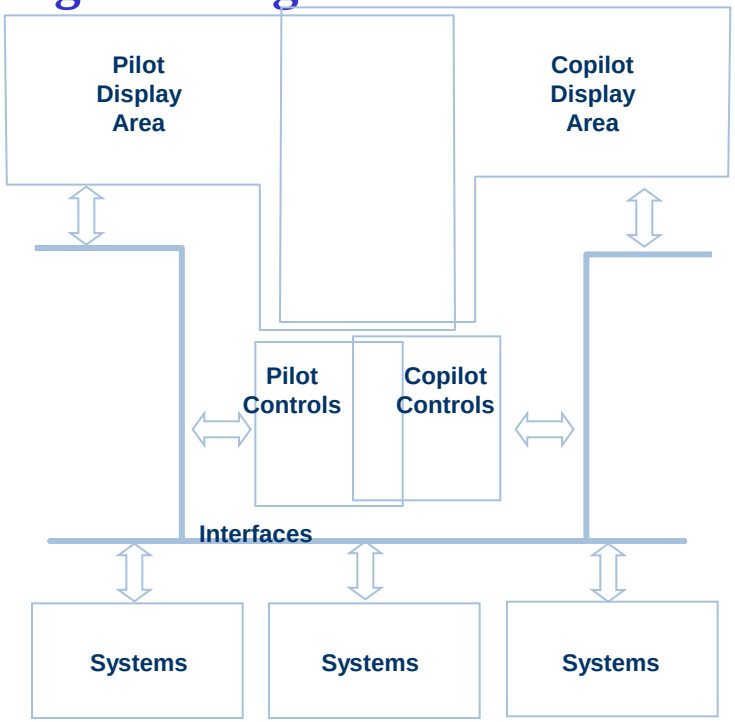
GEA Tianjin / 中国民航大学中欧航空工程师学院

Avionics Suite – Architecture Early Sketch



AC 25-11A Attitude Reqts ➔ Logical Design Rules

Failure Condition	Hazard Classification
Loss of all attitude displays, including standby display	Catastrophic
Loss of all primary attitude displays	Major – Hazardous(*)
Display of misleading attitude information on both primary displays	Catastrophic
Display of misleading attitude information on one primary display	Hazardous
Display of misleading attitude information on the standby display	Major
Display of misleading attitude information on one primary display combined with a standby failure (loss of attitude or incorrect attitude)	Catastrophic



GEA Tianjin / 中国民航大学中欧航空工程师学院

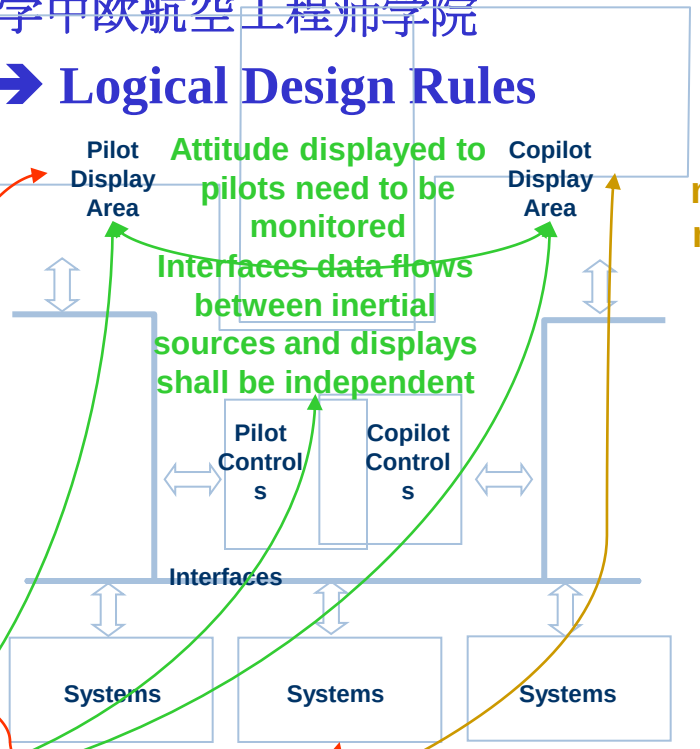
AC 25-11A Attitude Reqts ➔ Logical Design Rules

Interfaces shall guarantee independence between data flows to primary displays

At least 2 dissimilar types of display

At least 3 PFD displays (2 primary + Stby)
Additional PFD display and/or Stby for dispatch improvement

Failure Condition	Hazard Classification
Loss of all attitude displays, including standby display	Catastrophic
Loss of all primary attitude displays	Major – Hazardous(*)
Display of misleading attitude information on both primary displays	Catastrophic
Display of misleading attitude information on one primary display	Hazardous
Display of misleading attitude information on the standby display	Major
Display of misleading attitude information on one primary display combined with a standby failure (loss of attitude or incorrect attitude)	Catastrophic



Display need to be monitored

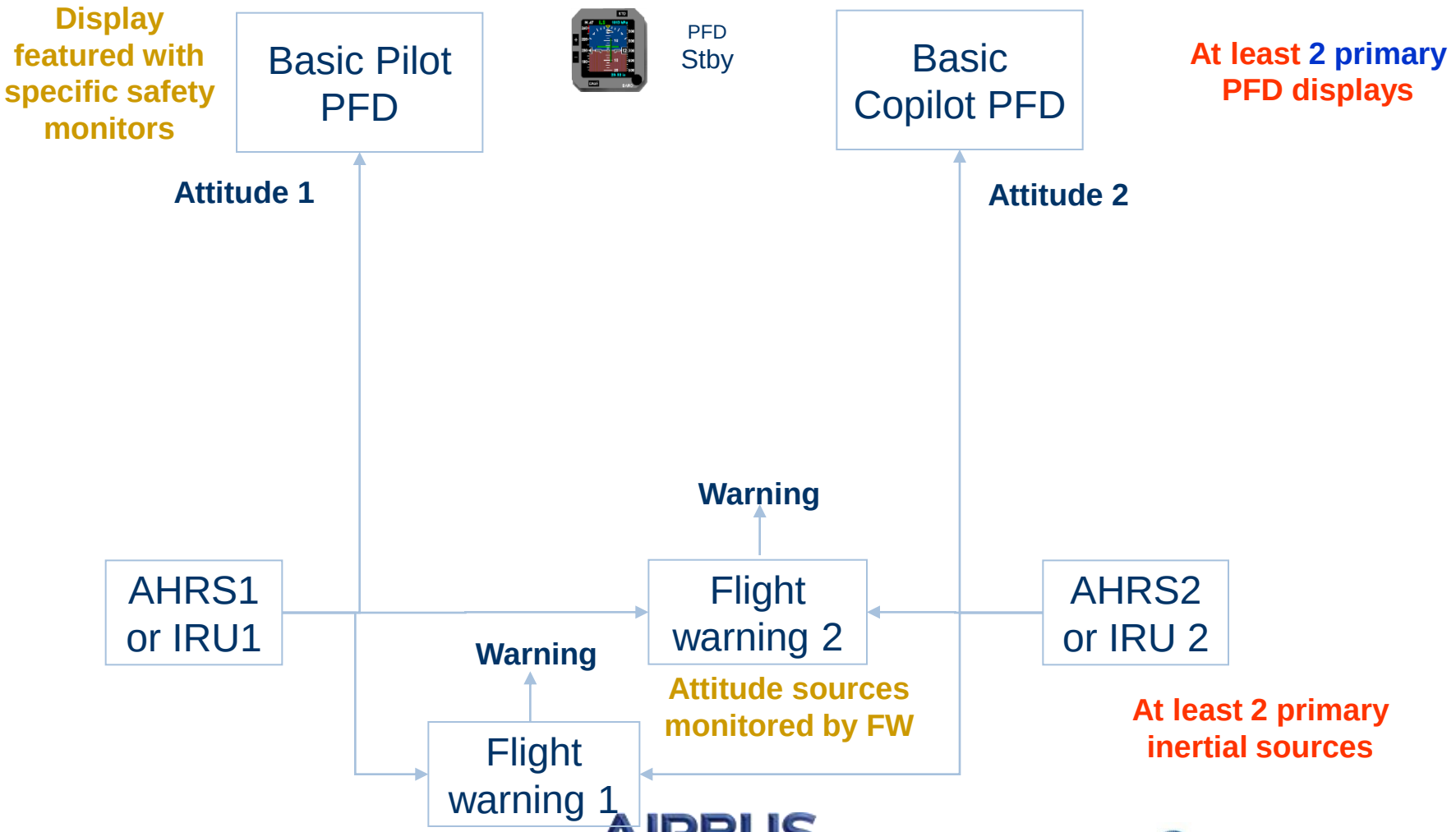
At least 2 dissimilar types of inertial reference

At least 3 inertial sources (2 primary + Stby)
A 3rd primary source and/or 2nd standby can be added for dispatch improvement

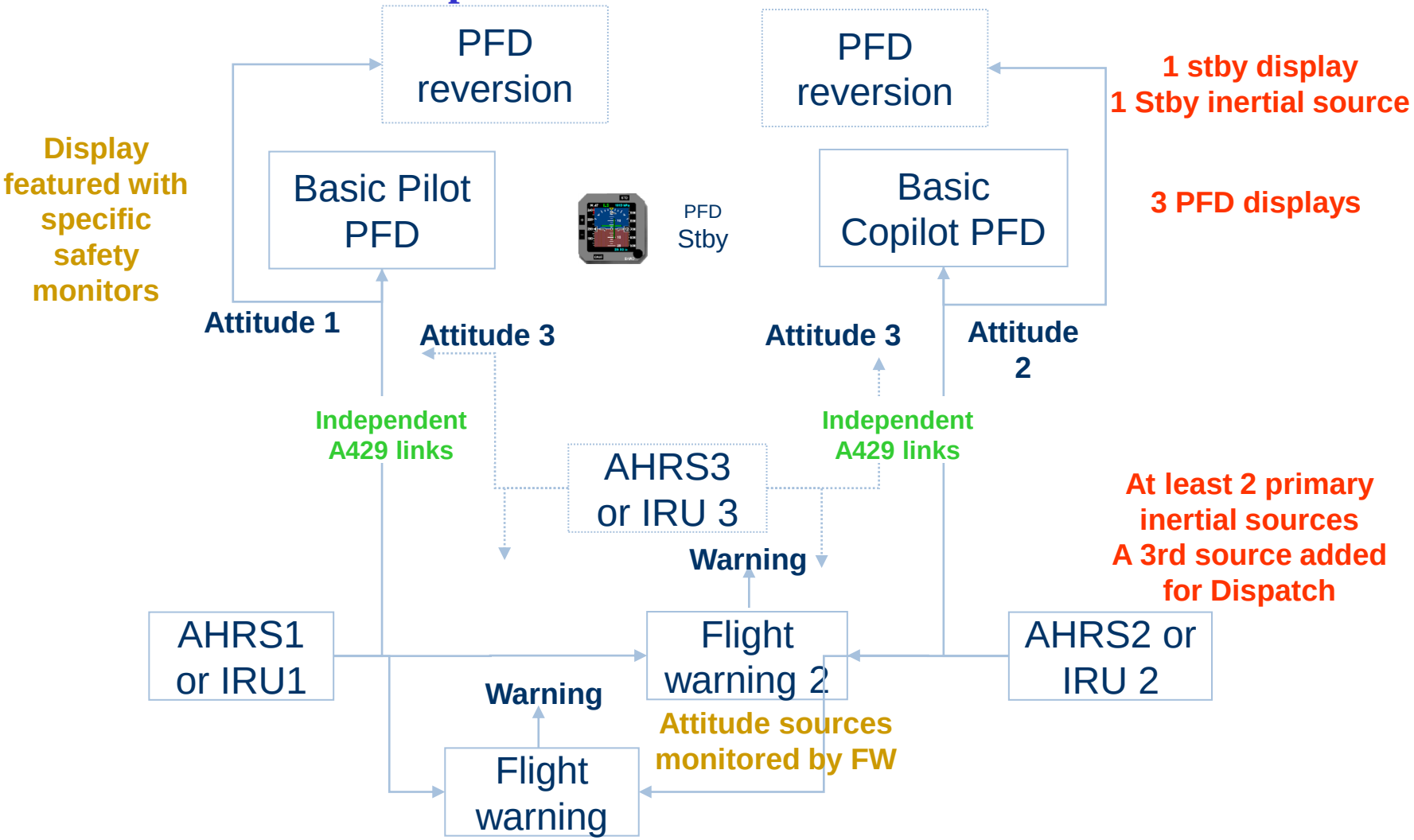
No need to monitor standby display or standby attitude

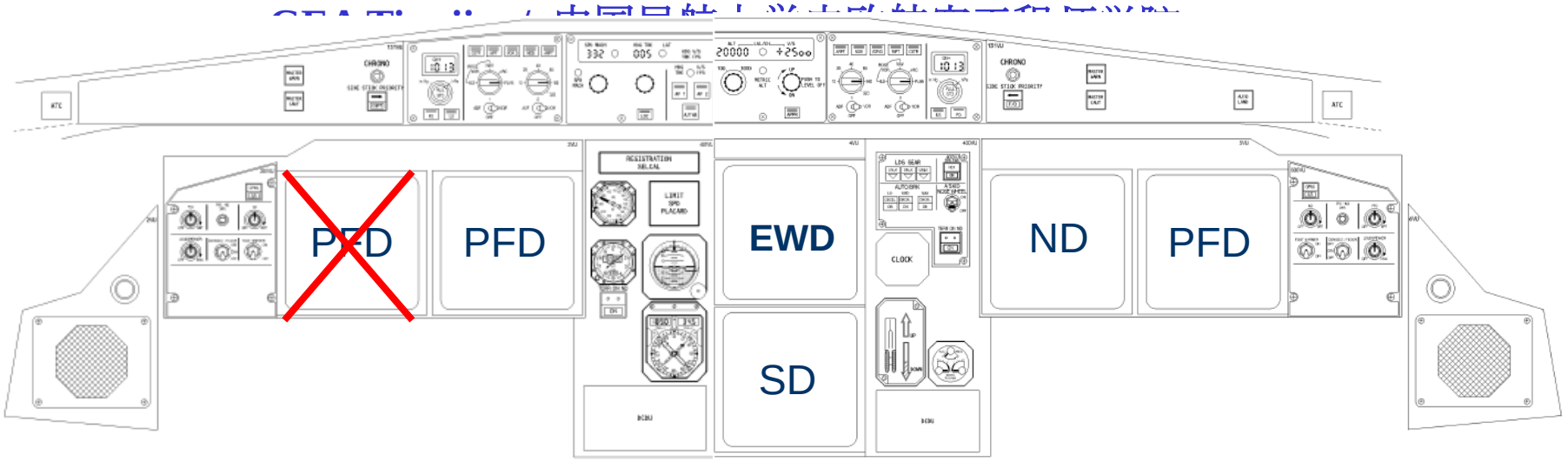
1 stby display (dissimilar from primary displays
1 Stby inertial source

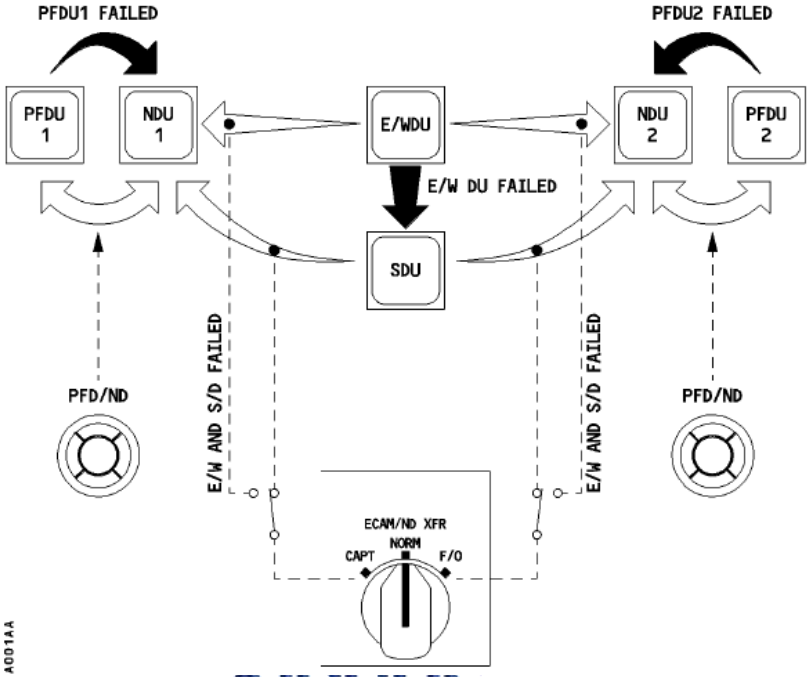
Basic Certification Architecture



Dispatch reliable architecture





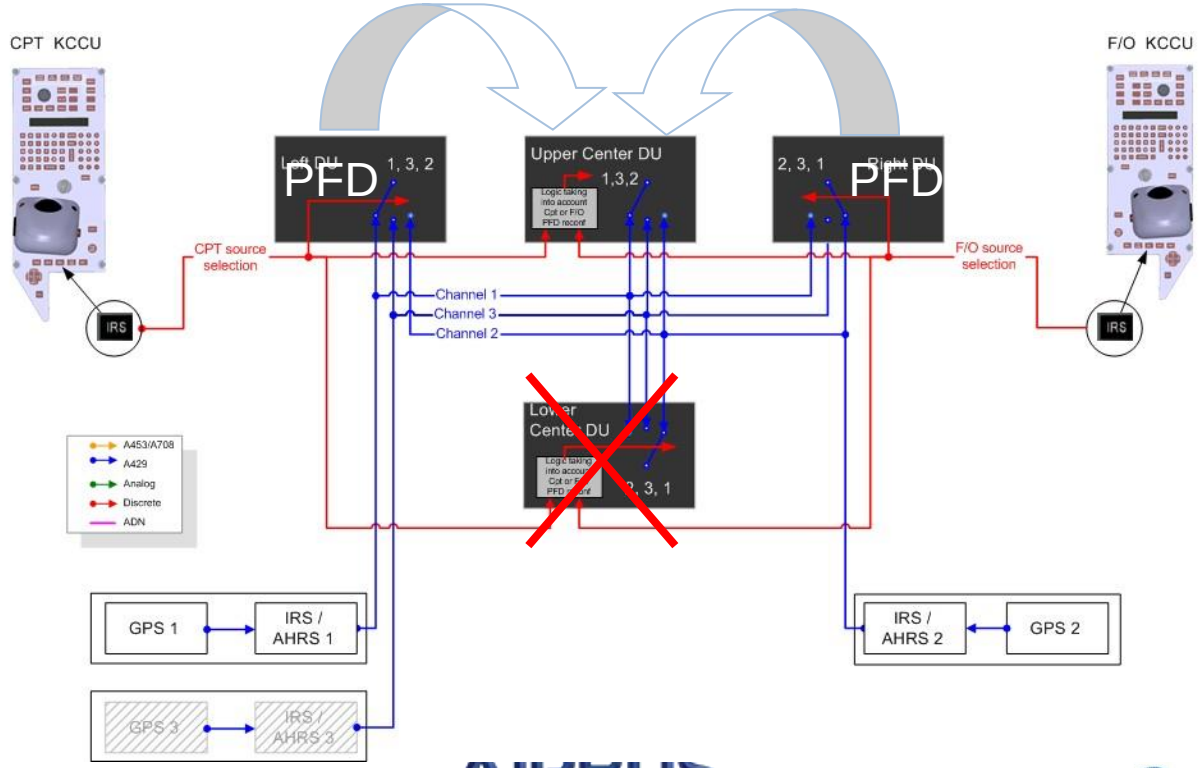


3 IRS directly interfaced to CDS

Airbus proprietary

GEA Tianjin / 中国民航大学中欧航空工程师学院

Example of Flight Deck under MMEL conditions



Agenda

- Avionics suite general context
- Architecture development process
- Architectural general aspects
  - Architecture main drivers
  - Variability analysis
  - Generational improvements
- Architectural building: addressing safety requirements
  - Architecture building rule-of-thumb
  - Safety requirements ←→ candidate logical architectures
- Architecture building examples
  - Display primary parameters

Thank you !