

# A holistic training on CERTIFICATION OF SOFTWARE (DO 178 C)

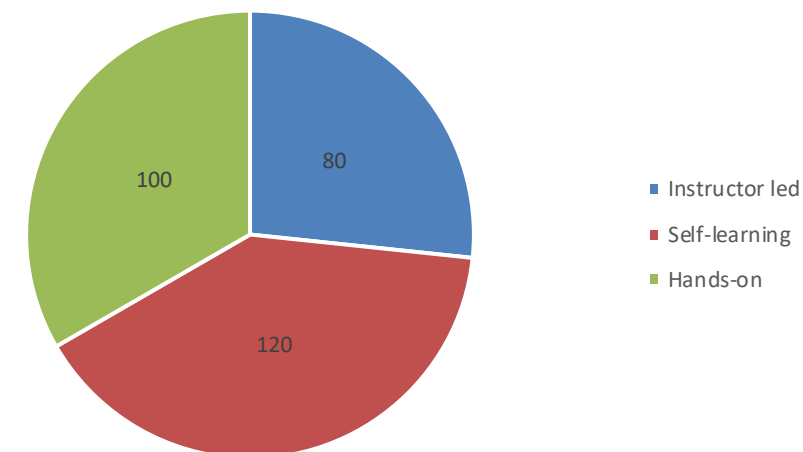
## Context setting and curriculum overview

**CLASS 1**

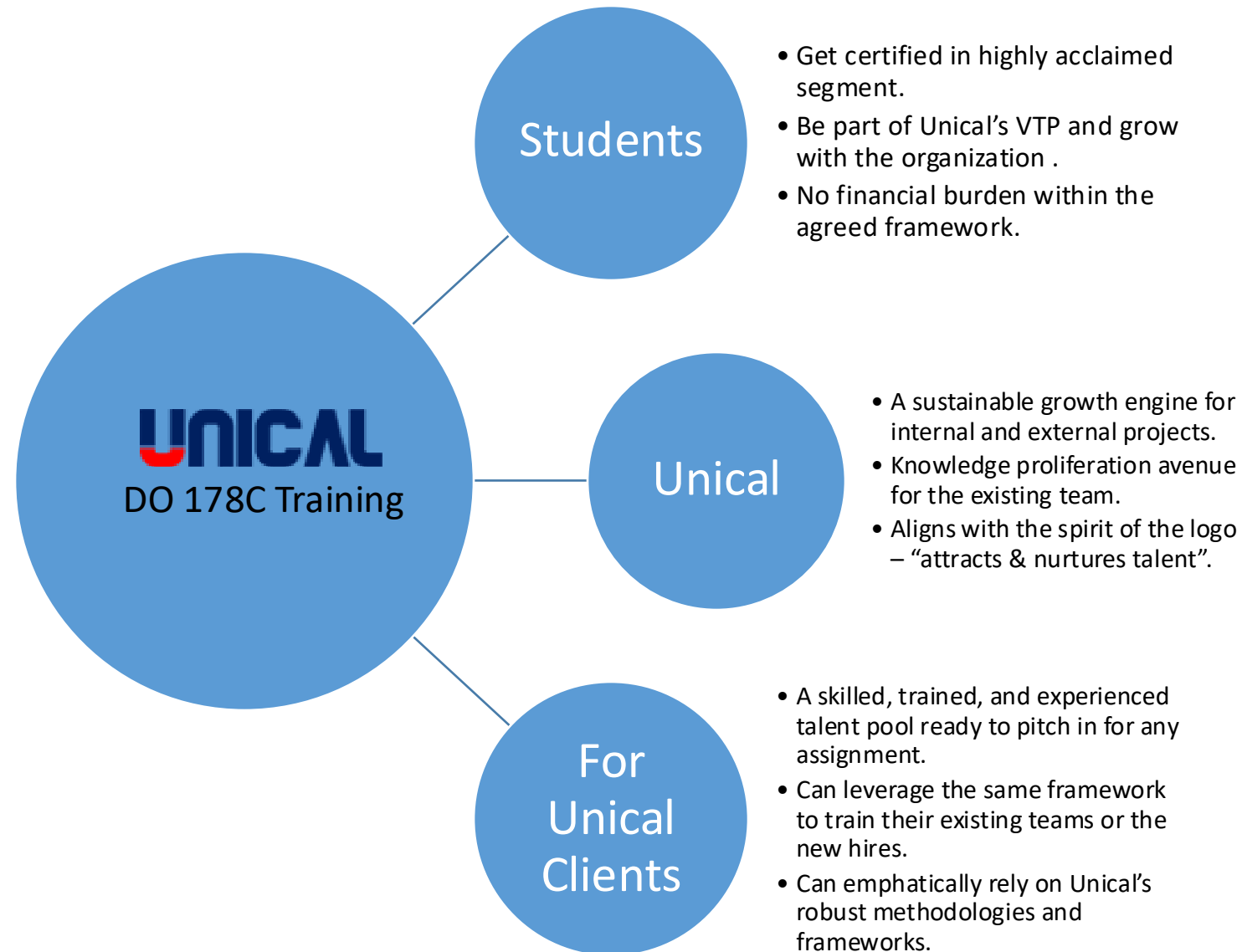
**At the end of this training session (300 hours), participants will be able to get an idea on–**

- Software certification overview – the happenings in India and around the world.
- Overview of Safety-critical systems and the high-level SDLC flow
- Four stage of involvement and the expectation for each stage
- Mandatory documents and the records
- Hands-on experience with common tools used for testing
- Supplementary information such as DO 330 and DO 331 to enhance the learning.

Training sessions distribution in hours



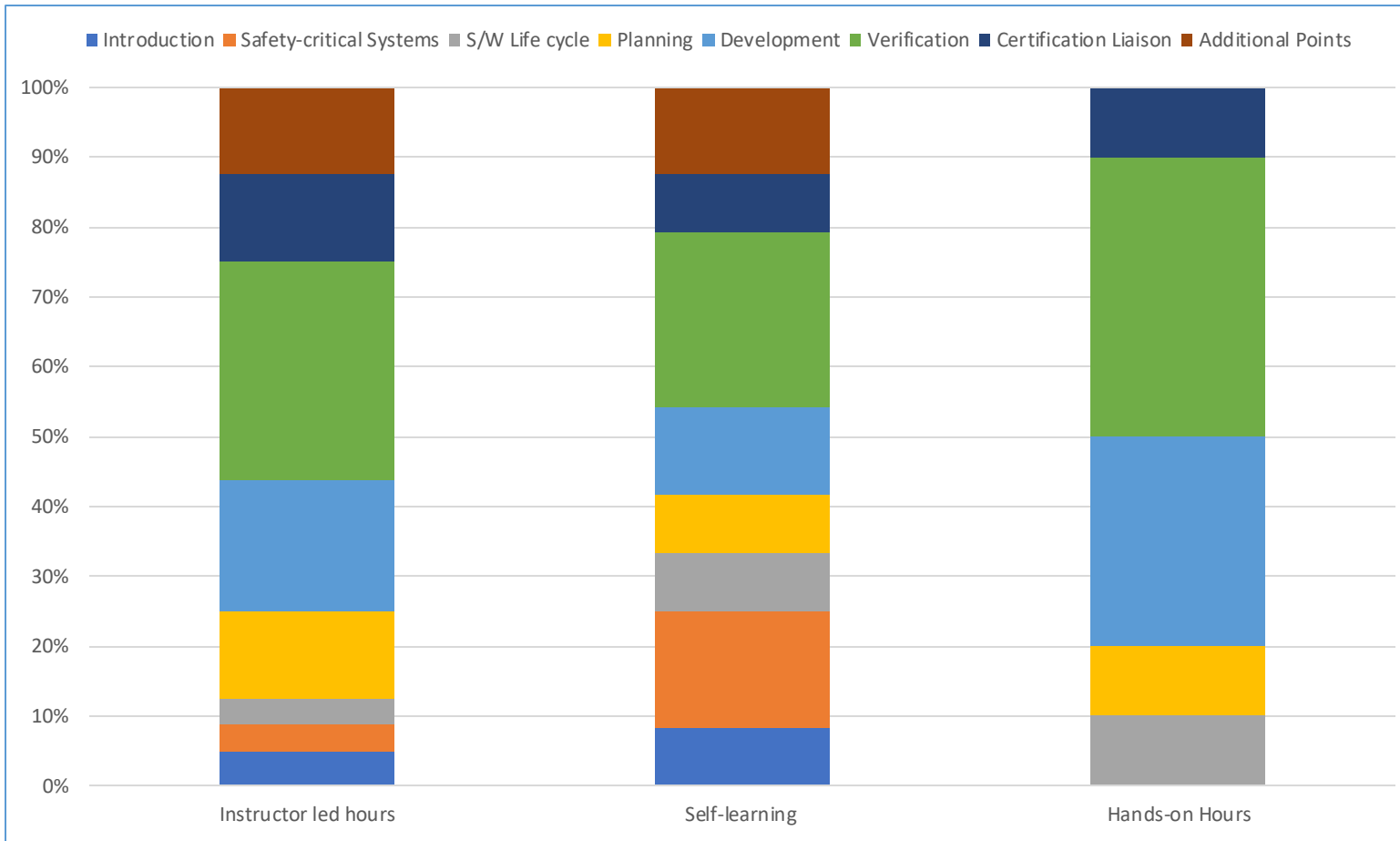
# The Advantages of this training



# 'Run Rules' of the training

- Don't miss any sessions, and be on time
- Minimize disruptions (cell phones and unwanted breaks/distractions)
- Ask Questions
  - Questions during sessions are welcome - only caveat is answers may have to be limited due to schedule
  - Instructors will be available through emails for individual questions
- Maintain an environment of mutual respect
- Have fun!

# How should you plan your time?



Let's go!!!

# Section wise Details - Introduction

- This is a 4 hours context setting session by the instructor, and after that you will be provided enough material and reference links to explore on your own.
- You are expected to spend at least 10 hours of self-learning to get well-versed with the topics covered in this section.
- Though this section is relatively short, this covers the entire landscape of the course curriculum, including the areas that need to be focused, and the opportunities that can be explored. The key topics covered are –
  - DO 178C Overview
  - India Airworthiness policies and procedures
  - Brief on world-wide certifying agencies
  - A quick glance of other related/connected standards

- Software is a part of the larger system. A system consists of several modules, line replicable units etc. The main objective of this section is to give overview of a system and general aspects of common LRUs such as control systems, power systems, navigation systems etc.
- By getting the mastery of this section, you will be better positioned to interact with other subject matter experts from mechanical, aero engineering etc. that deal with you the Software professionals.
- The key topics covered are –
  - Air systems classification and safety categorization
  - Three levels of LRUs
  - Software Vs Safety-critical Software – key points to ponder
  - Brief on STLC walkthrough for safety-critical systems

- While the first two sections dealt only with the context setting, this section enables you to launch the prolific career in Airworthiness and Software aspects of airworthiness.
- This is a mind-refresh section for the students who come from Software background. For others, this briefs about the entire Software Development Life Cycle (SDLC) phases and the activities
- The topics covered in this section are –
  - The traditional V-Process model
  - Importance of ETVXIO criteria for each phase
  - Overview of other SDLC processes
  - Briefly on Agile Methodology and Software Project Management.
  - The common issues, challenges, and the problems.



- This phase can be considered “first term” exam in DO 178C process. This phase deals with the SOI-1 assessment aka Stage of Involvement -1.
- The topics covered in this section are –
  - Software Planning Process Objectives
  - Software Plans
  - Applicable Standards
  - Other aspects of Planning

- This section should be looked from “developer” perspective. The development aspects starting from getting the requirements, requirements to the developed code block get covered with the practical aspects and focusing on potential issues and challenges during the development phase, particularly on stakeholder management.
- The topics covered in this section are –
  - Requirements Process
  - Design Process
  - Coding Process

- This can be considered most important section in this training with substantial learning that includes self-learning as well as the expected hands-on practices.
- The topics covered are –
  - DO 178C Testing guidelines
  - Test Coverage Analysis
  - Importance of Traceability
  - Static Analysis Tools
  - Third-party and Object Code Testing

- This is the crucial section. This can be attributed as “final exam” preparation for any company. The consolidated and compiled reports of all three previous stages and required additional reports and details will be discussed in this section.
- The topics covered in this section are –
  - Stakeholders Expectation and Final Certification
  - Full story – planning to the final compliance substantiation.
  - Software Accomplishment Report
  - DO 178 C Table A-10: Objectives 1, 2, and 3.

# Additional Points & Wrap-up

- This section focuses on the connected points that come in overall ecosystem of Software Airworthiness.
- This section is expected to be more interactive in which the students are expected to get the required clarity on the topics covered, potential roadmap for their careers, and get ready for the final certification.
- The topics covered in this section are –
  - Software Configuration Management
  - Software QA and QC Activities
  - DO 178 C Supplements – DO 330, 331, 332, and 333.
  - Wrap-up and inputs on Unical Assessment Test.



# A holistic training on CERTIFICATION OF SOFTWARE (DO 178 C)

Airworthiness – IMAP, ITAR, and more

**CLASS 2**

# Airworthiness certification overview

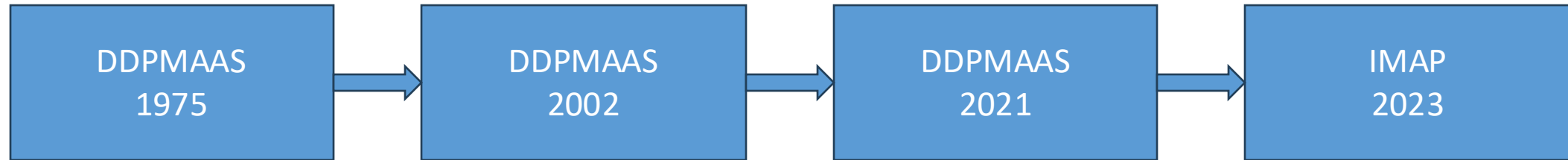
- Certification must happen concurrently and progressively.
- The certification can be categorized into four stages -
  - Design evaluation
  - Ground testing
  - Flight testing
  - Certification
- The overall certification is addressed at three levels -
  - LRU level - initial
  - System level - integrated
  - Overall Aircraft level - final

# Planning and Design Evaluation

- Preliminary design reviews / Critical design reviews focus on -
  - System description
  - Conduct of the review
  - Performance
  - Schedule
  - Technical risks, issues and opportunities
  - Establishment of the baseline
  - Design considerations
  - Conclusion
- Various reviews
  - Flight development program review
  - Design, development certification review
  - Design production and quality review
  - Flight test requirement generation and certification
  - Technical control group



# Policies and procedures in India

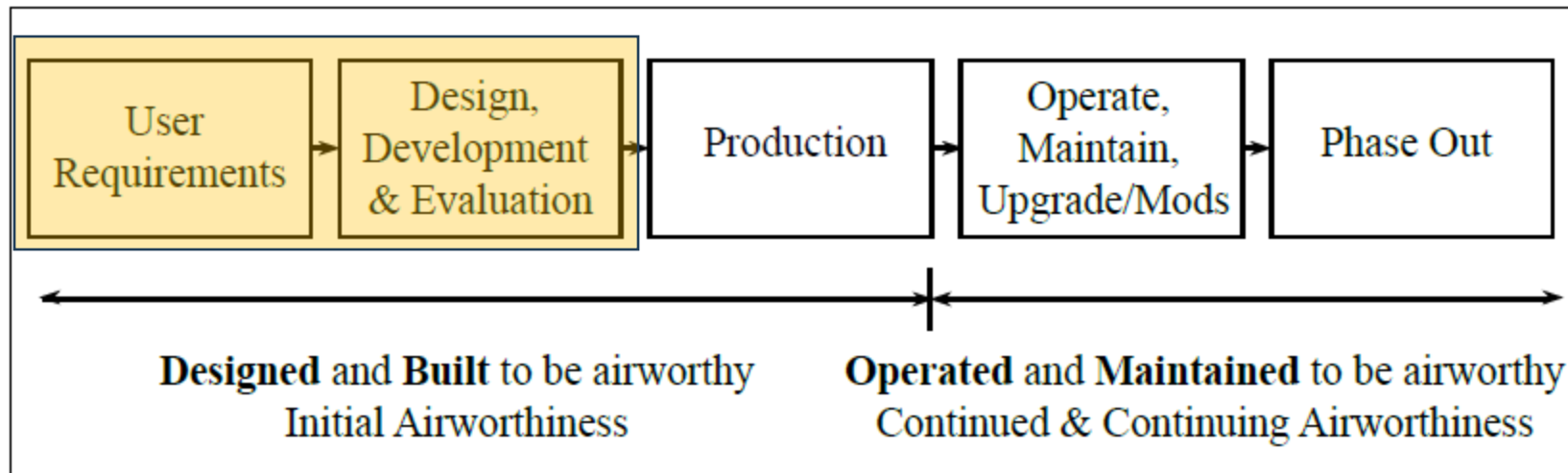


- Deals with –
  - Policies, Regulations, and Manuals
- Consists of –
  - Airworthiness Management Framework
  - Design, Development, Production, and Certification
  - Ab-initio Development
  - Templates and guidelines

- Procedural document on Technical Airworthiness, covering roles and responsibilities and the empowerment of the stakeholders to ensure airworthiness of Indian Military Air Systems.
- An overview-
  - The same DDP MAS – with enhanced inputs gives more clarity on three types of acquisitions
  - Revised various templates and forms.
  - Three types of acquisitions as part of new nation-wide pitch –
    - Buy; buy and make; make.
  - Design Organization Approval (DOA) – CEMILAC
  - Production and Maintenance Organization Approval – DGAQA
- Part-1 consists of three chapters, the present introduction chapter, the military airworthiness framework chapter and the military acquisitions chapter.
- Part-2 consists of 12 chapters to exclusively cover the airworthiness procedures for Ab-initio development, License production etc.
- In summary, the activities related to design, development, manufacture and procurement of Air System / Airborne Stores for the Indian Military, shall follow the procedures as outlined in the applicable chapters of this IMAP-2023 document

# Indian Military Airworthiness Framework

- Airworthiness is a concept, the application of which ensures that the condition of an Air System is suitable to safely carry out the mission for which it has been designed, built, maintained and operated.
- To fulfill the airworthiness, two aspects are important - (i) technical airworthiness - air systems are designed, developed, produced, and maintained to the approved airworthiness criteria. (ii) operational airworthiness - air systems are serviced, maintained, and operated as per the defined criteria.



- Airworthiness requirements are based on Indian Military Technical Airworthiness Requirements (IMTAR -21)

# Few critical definitions before we start our journey

- **Safety:** Freedom from those conditions that can cause death, injury, illness, damage to or loss of equipment or property, or environmental harm".
- **Safety-critical software** includes software whose operation or failure to operate can lead to a hazardous state, software intended to recover from hazardous states, and software intended to mitigate the severity of an accident.
- **"Airworthiness"** means the continued capability of the military air systems and airborne stores to perform satisfactorily and fulfil mission requirements, throughout the specified life in the specified environments with acceptable levels of safety and reliability.
- **"Aircraft"** means any machine which can derive support in the atmosphere from reactions of the air other than reactions of the air against earth's surface and includes balloons, whether fixed or free, airships, kites, gliders, and flying machines.
- **"Air-system"** include fixed or rotary wing aircraft, unmanned aircraft, air launched missiles, and aero engines.
- **"Airborne stores"** include all parts and appliances and their associated **Software**, Firmware, Propeller, Aero Materials, Air Armaments, Equipment"
- **"Aeronautical related stores"** includes ground support equipment, simulators, test rig, power supply, hydraulic trolleys, arrester barriers etc.

## Certification of Ab-initio Design and Developed Air borne Software

The approach to clearance shall be in accordance with CEMILAC regulations.

(A) The clearance process comprises the following major steps:

- i. Determination of Software Criticality Level based on System Safety Assessment
- ii. Identifying the system requirements allocated to Software
- iii. Agreement with Software Certification Plan (SCP) and other plans
- iv. The approach to clearance shall be in accordance with Subpart in the subsequent sections.
- iv. Verification of Software Requirements
- v. Verification of Software Design and implementation
- vi. Conduct of Software Evaluation
- vii. Demonstration of compliance with SCP and review of Certification
- viii. Issuance of Software Clearance

(B) Successful completion of certification process for an Airborne Software v in CEMILAC issuing a Software Clearance, based on the application/re software clearance from the Main Contractor.

# Steps to apply for CEMILAC certification

The following need to be submitted -

- a. A description of the firm
- b. A description of the software being developed / functional requirement specification.
- c. Scope of the program
- d. Timelines of the program
- e. Criticality classification of the Software
- f. Standard compliance mandated by the user, if any
- g. Intended end use platform (if available)
- h. Any special conditions.

## Acceptable means of compliance

- a. Composition of the IV&V team shall be based on the criticality level of the software under evaluation.
- b. IV&V team shall consist of system experts, domain experts, testing experts from relevant stake holder organizations, CEMILAC and DGAQA representatives.
- c. IV&V team shall be independent from the software design and development team.
- d. IV&V team shall carry out IV&V planning, carry out independent reviews, analysis verification, testing reporting activities and participate in Software review meetings, during the various phases of Software life cycle
- e. IV&V recommendation is required input for CEMILAC for Software clearance.
- f. CEMILAC has got the prerogative to create an evaluation team to augment the efforts of certification.

# The aspects that you need to focus are

- System Requirements and criticality level
- Identification
- Constitution of Software IV&V Team
- Software Certification Plan
- Software Planning
- Software Requirement Analysis
- Software Preliminary and Detailed Design Reviews
- Software Code Analysis
- Module Level Testing
- Integration Testing
- Software Verification and Validation
- Software Quality Assurance
- Software Configuration Management
- Clearance for Airborne Software
- Clearance of Software Modification after initial approval



# A holistic training on CERTIFICATION OF SOFTWARE (DO 178 C)

## Overview of DO-178 C

### **CLASS 3**

# Introduction to DO 178 C

- DO-178C is a software produced by Radio Technical Commission of Aeronautics Inc. (RTCA), used for guidance related to Equipment certification and software consideration in airborne systems. RTCA has no longer a “valid” full form.
- DO-178C is mainly divided into 5 major processes -
  - Software Planning
  - Software Development
  - Software Verification
  - Software Configuration Management
  - Software Quality Assurance

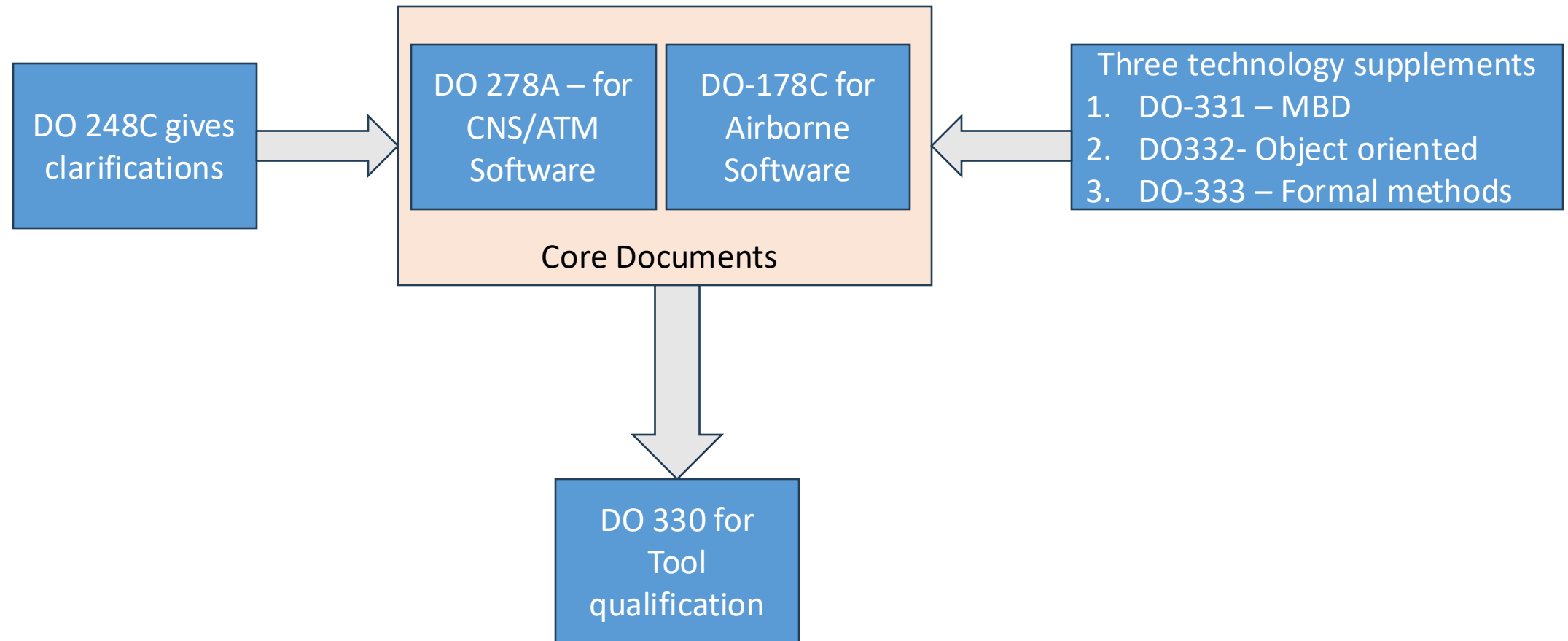
# The challenges

- Though historically, safety-critical software has been quite respectable. There could be potential challenges going forward due to following reasons -
  - Increased lines of code – more Software is coming into the systems
  - Increased complexity – different federated hardware etc.
  - Increased criticality- What used to be mechanical is going towards Software.
  - More with less – Economics are driving the overall delivery
  - Increased outsourcing – For various reasons, also a cause.
  - Attrition of experienced engineers
  - Lack of available training

# Chronological progress

Evolution of DO-178B and Related Documents		
Document	Year Published	Content
DO-178	1982	Provides basic information for developing airborne software.
DO-178A	1985	Includes strong software engineering principles. Includes verification and validation of requirements.
DO-178B	1992	Significantly longer than DO-178A. Provides guidance in form of objectives, rather than "how". Provides visibility into life cycle process and data. Does not include requirement validation.
DO-248B	2001	Includes errata of DO 178B. Provided FAQs.
DO-278	2002	DO-178B applicability to CNS/ ATM software.
DO-178C	2011	Very similar to DO-178B. However, clarifies several areas, adds guidance for parameter data items, and references DO-330 for tool qualification.
DO-278A	2011	Stand-alone from DO-178C, unlike DO-278 which made direct references to DO-178B. Very similar to DO-178C.
DO-248C	2011	Updated DO-248B to align with FAWs
DO-330	2011	Provides guidance on tool qualification
DO-331	2011	Provides guidance on MBD AND VERIFICATION
DO-332	2011	Provides guidance on OOT & RT
DO-333	2011	Provides guidance on formal methods.

# Pictorial view



# 12 Sections of DO-178C

- Section 1: Introduces DO 178C
- Section 2: Briefs on framework aligns with ARPA4754A
- Section 3: Briefly covers life cycle processes – all four COIs, CM, and QA.
- Section 4: Planning process objectives
- Section 5: Development process objectives
- Section 6: Verification process. Includes, reviews, analysis, and tests.
- Section 7: Software configuration management process
- Section 8: Guidance for quality assurance process
- Sections 9 & 10: Certification liaison process
- Section 11: Identifies the life cycle data generated
- Section 12: Additional considerations – tools, alternative methods etc.

# Do 178C Design Assurance Levels

- DO-178 C Design Assurance Levels –
  - DAL A: Catastrophic failure rate of  $\leq 1 \times 10^{-9}$  and 71 objectives
  - DAL B: Hazardous failure rate of  $\leq 1 \times 10^{-7}$  and 69 objectives
  - DAL C: Major failure rate of  $\leq 1 \times 10^{-5}$  and 62 objectives
  - DAL D: Minor failure rate of  $1 \times 10^{-5}$  and 26 objectives
  - DAL E: No failure rate condition or objectives and no safety effect

DAL	A	B	C	D	E
<b>Planning Artifacts</b>					
PSAC	X	X	X	X	
SDP	X	X	X	X	X
SVP	X	X	X	X	X
SCMA	X	X	X	X	X
SQAP	X	X	X	X	X
SW Req Standards	X	X	X		
SW Design Standards	X	X	X		
SW Code Standards	X	X	X		
<b>Development Artifacts</b>					
SW H/L Requirements	X	X	X	X	X
SW Design Description	X	X	X	X	X
SW L/L Requirements	X	X	X		
<b>SW Verification Artifacts</b>					
SW Verif C&P	X	X	X	X	X
SW Verification Results	X	X	X	X	X
Trace Data	X	X	X	X	X
Source Code	X	X	X		
Executable Object Code	X	X	X	X	X
Parameter Data Item File	X	X	X	X	X
<b>SW CM and SQA Artifacts</b>					
SCM Records	X	X	X	X	X
SW Config. Index	X	X	X	X	X
Problem Reports	X	X	X	X	X
SW Life Cycle Env Config Index	X	X	X	X	X
SQA Records	X	X	X	X	X
<b>Certification Liaison Process</b>					
SW Accomplishment Summary	X	X	X	X	

# Do 178C Annex A Tables – a summary

Summary of DO-178C Annex A Tables		
Table #	Objectives	Annex A Table Title
A-1	7	Software planning process
A-2	7	Software development process
A-3	7	Verification of outputs of software requirements process
A-4	13	Verification of output of software design process
A-5	9	Verification of outputs of software coding and integration process
A-6	5	Testing of outputs of integration process
A-7	9	Verification of verification process results
A-8	6	Software configuration management process
A-9	5	Software quality assurance process
A-10	3	Certification liaison process



# All in one Table!!!

Overview of Software Life Cycle Data		
DO-178C Section	LC Data Item	Annex A Table Title
11.1	Plan for Software Aspects of Certification	Top level software plan used to document agreements with the certification authority
11.2	Software Development Plan	Describes software development procedures and life cycle to guide the dev team and ensure compliance to DO-178C dev objectives
11.3	Software Verification Plan	Describes software verification procedures to guide the verifiers and to ensure DO-178C compliance
11.4	Software Configuration Management Plan	Establishes the software configuration management environment, procedures, activities, and processes to be used throughout the software development and verification effort
11.5	Software Quality Assurance Plan	Establishes the plan for software quality assurance's oversight of the project to ensure compliance to DO-178C objectives and the plans and the standards.
11.6	Software Requirements Standards	Provides guidelines, methods, rules, and tools for the requirements authors
11.7	Software Design Standards	Provides guidelines, methods, rules, and tools for the designers
11.8	Software Code Standards	Provides guidelines, methods, rules, and tools for using the programming language effectively
11.9	Software Requirements Data	Defines the high-level and derived high-level software requirements
11.10	Software Design Description	Defines the software architecture, low-level requirements, and derived low-level requirements
11.11	Source Code	Consists of code files that are used together with the compile, link, and load data to create the executable object code and integrate it into the target computer.
11.12	Executable Object Code	The code that is directly read by the target computer's processor
11.13	Software Verification Cases and Procedures	Details how the software verification processes are implemented
11.14	Software Verification Results	The output of the verification processes
11.15	Software Life-cycle Environment Configuration Index	Identifies the software environment, including any tools used to develop, control, build, verify, and load the software
11.16	Software Configuration Index	Identifies the configuration of the software product, including source code, executable object code, and supporting life cycle data. Also includes build and load instructions
11.17	Problem Reports	Identifies product and process issues in order to ensure resolution
11.18	Software Configuration Management Records	Includes results of the various software configuration management activities
11.19	Software Quality Assurance Records	Includes results of the software quality assurance activities, including the software conformity reviews
11.20	Software Accomplishment Summary	Summarizes the compliance to DO-178C, any deviation from the PSAC, software characteristics, and open problem reports
11.21	Trace Data	Provides evidence of traces between requirements, design, code, and verification data
11.22	Parameter Data Item File	Includes data (such as configuration data) directly usable by the target computer's processor.

# A holistic training on CERTIFICATION OF SOFTWARE (DO 178 C)

## Aerospace Systems – a quick refresher

### **Lecture 4**

# Various Systems

Aircrafts

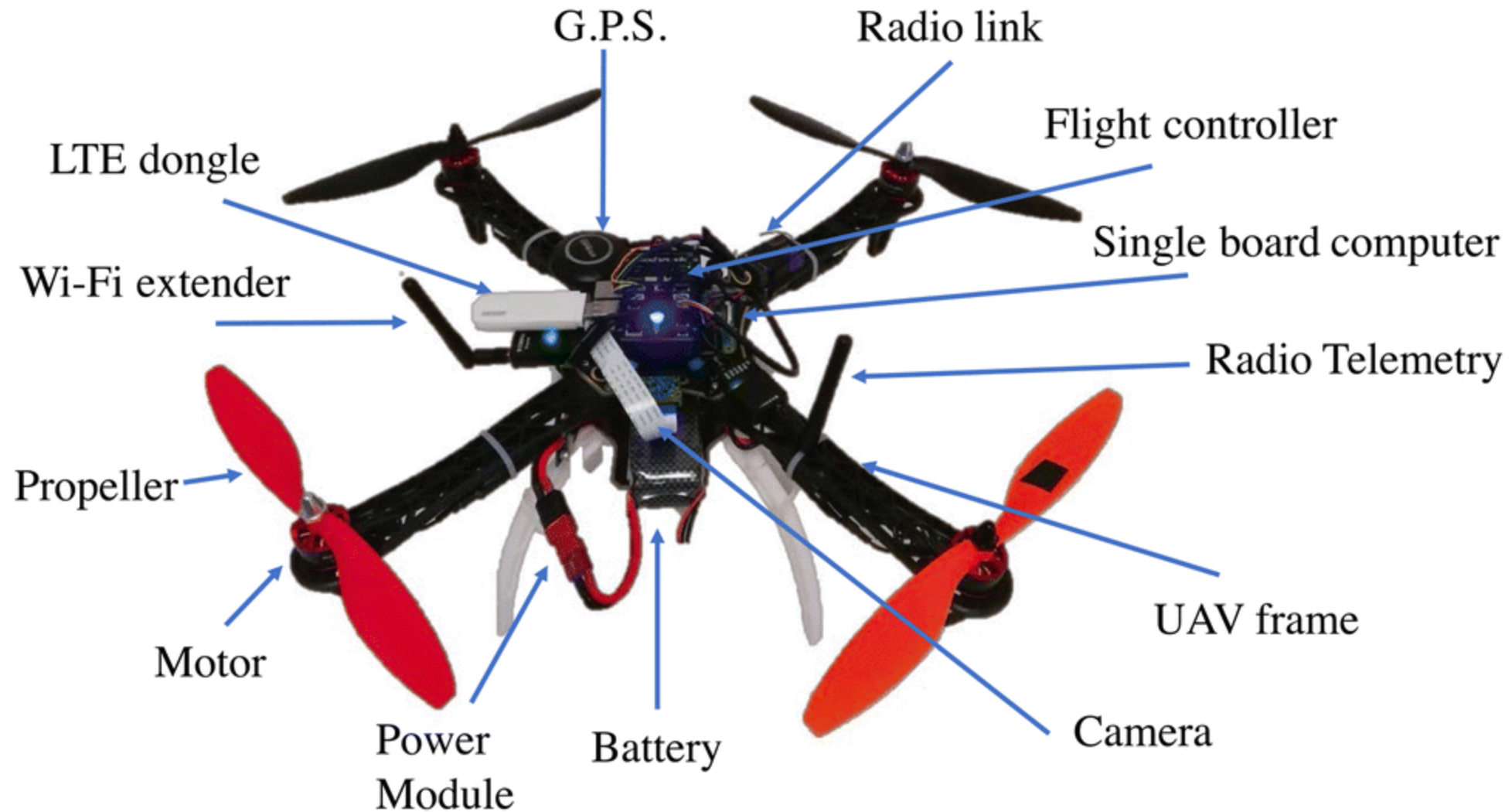
Drones

Missile Systems

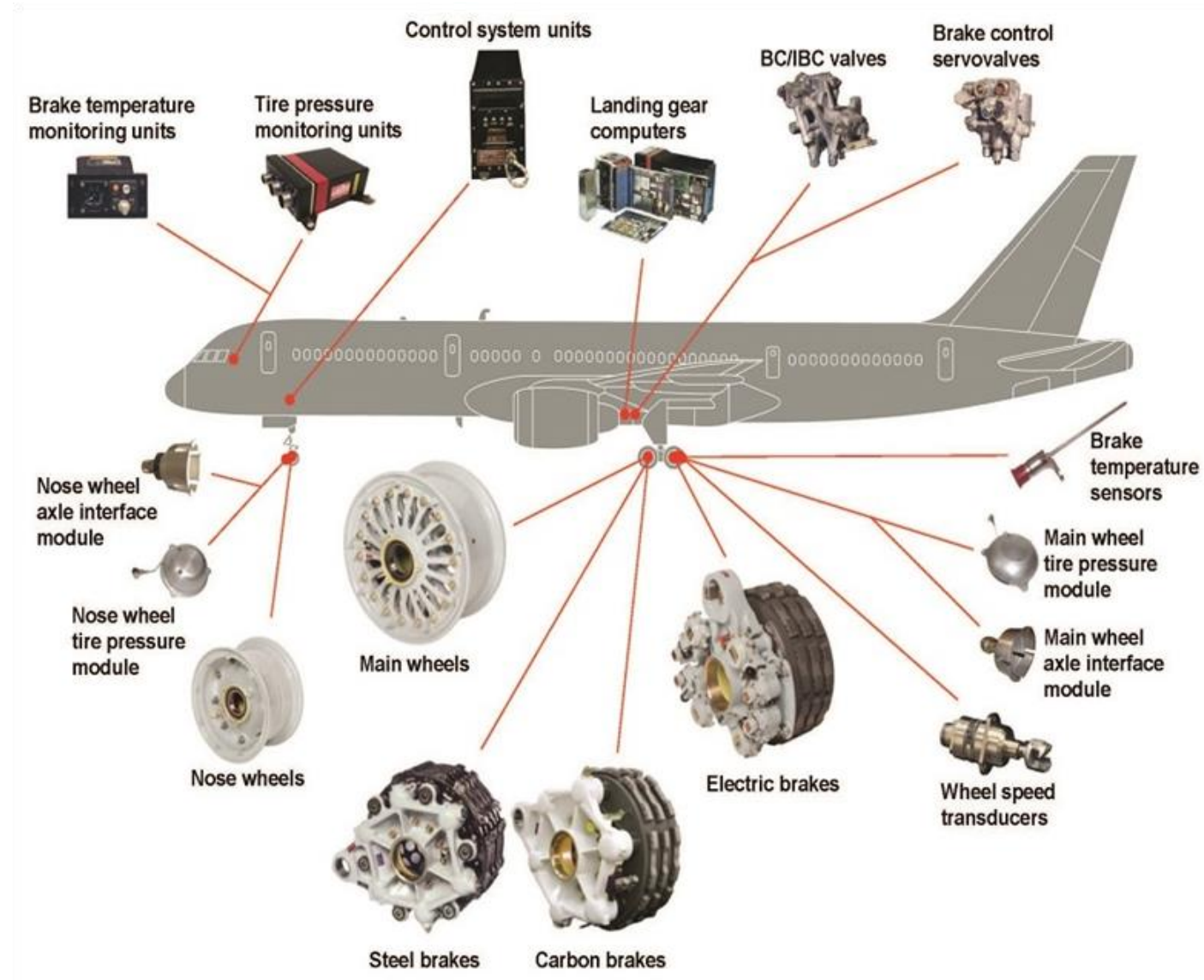
# Common LRUs

Level	Aircraft	Rocket	Missile
Level A	Flight Control Computers	Guidance and Control Systems:	Guidance and Control Systems
	Engine Control Units (ECUs)	Propulsion Systems	Seeker Heads
	Primary Flight Displays (PFDs)	Flight Termination System (FTS)	Infrared (IR)
	Multi-Function Displays (MFDs)	Gyroscopes	Radar
	Inertial Navigation Systems (INS)	Accelerometers	Warhead Activation Systems
	Global Positioning System (GPS) Receivers	Inertial measurement units (IMUs)	Fuzes
	Radar Systems:	Flight control computers	Detonators
	Air Data Computers (ADCs)	Control Surface Actuators	Arming mechanisms
Level B	Hydraulic System Components	Telemetry Systems	Propulsion Systems
	Electrical Power Distribution Units	Avionics Systems	Data Links
	Environmental Control Systems	Payload Separation Mechanisms	Inertial Navigation Systems (INS)
	Landing Gear Control Units	Stage Separation Systems	Power Systems
	Fuel Quantity Measurement Systems		Environmental Control Systems
	Emergency Locator Transmitters (ELTs)		
Level C	Passenger Entertainment Systems:	Environmental Control Systems	Telemetry Systems
	Galley Systems	Power Distribution Units	Structural Components
	Cabin Lighting Systems:	Thermal Protection Systems	Test Equipment Interfaces
	Lavatory Systems:	Payload Interface Systems:	

# Drones - Functional Blocks

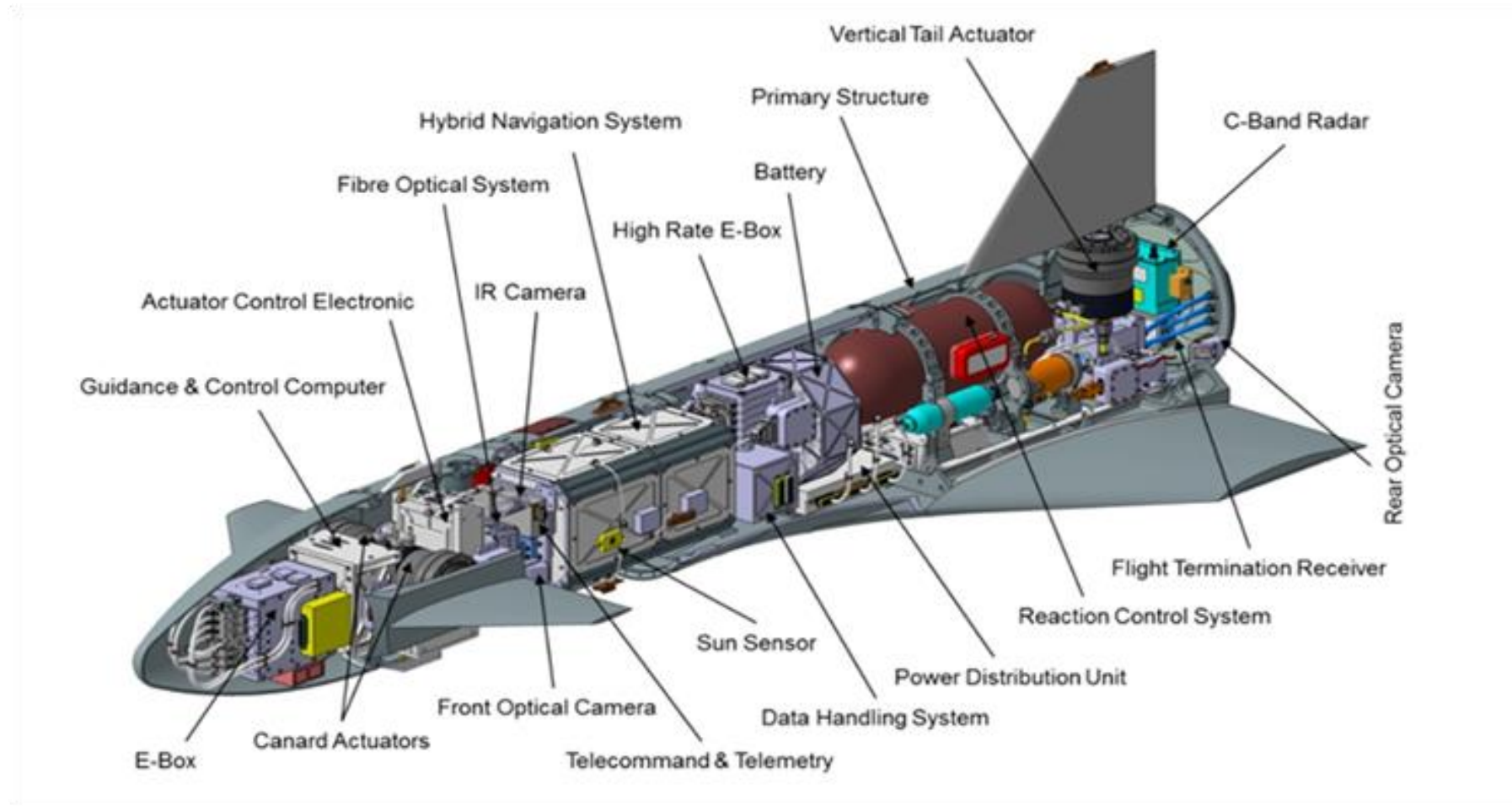


# Aircraft - Functional Blocks

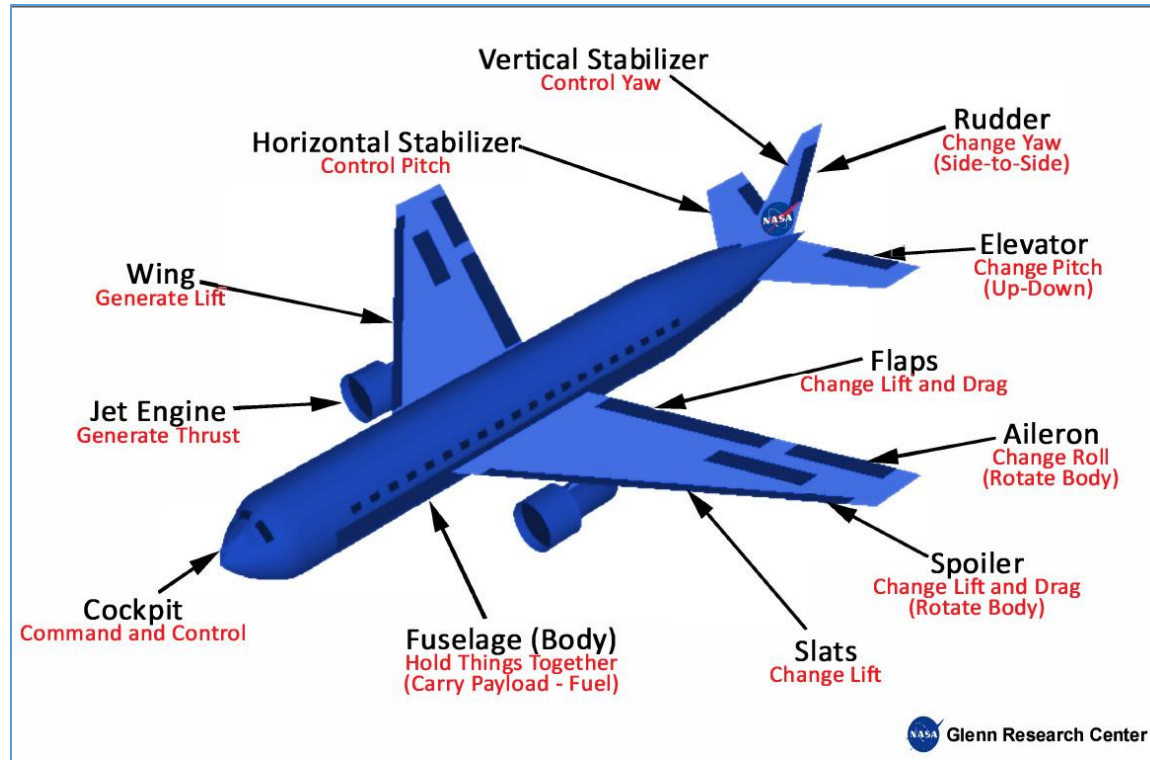




# Missile - Functional Blocks



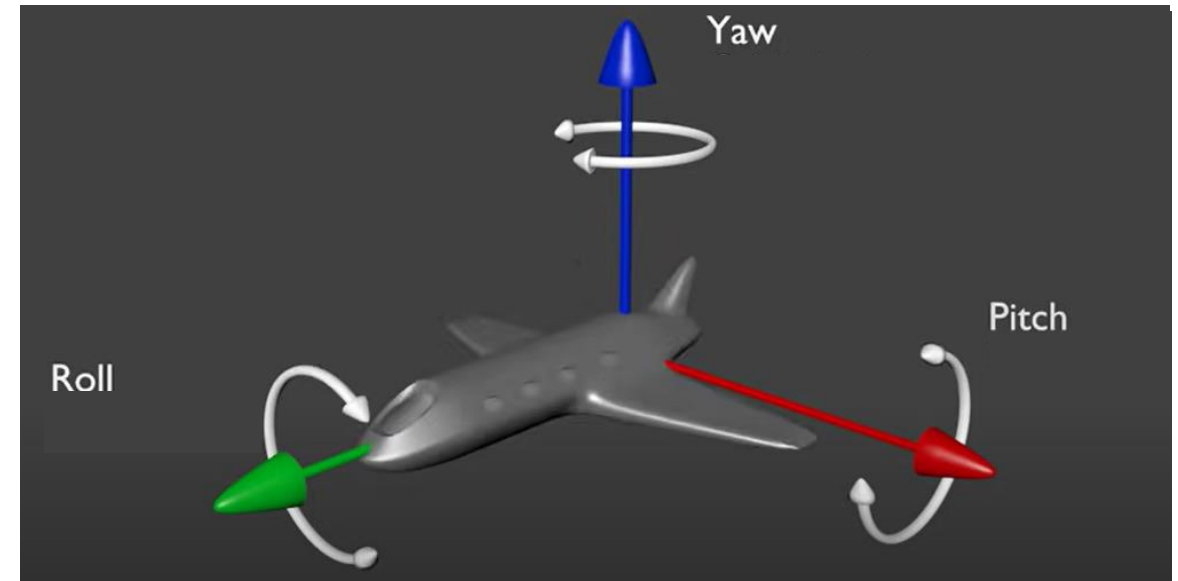
# Basic Aerodynamics



## The various stresses on an Aircraft

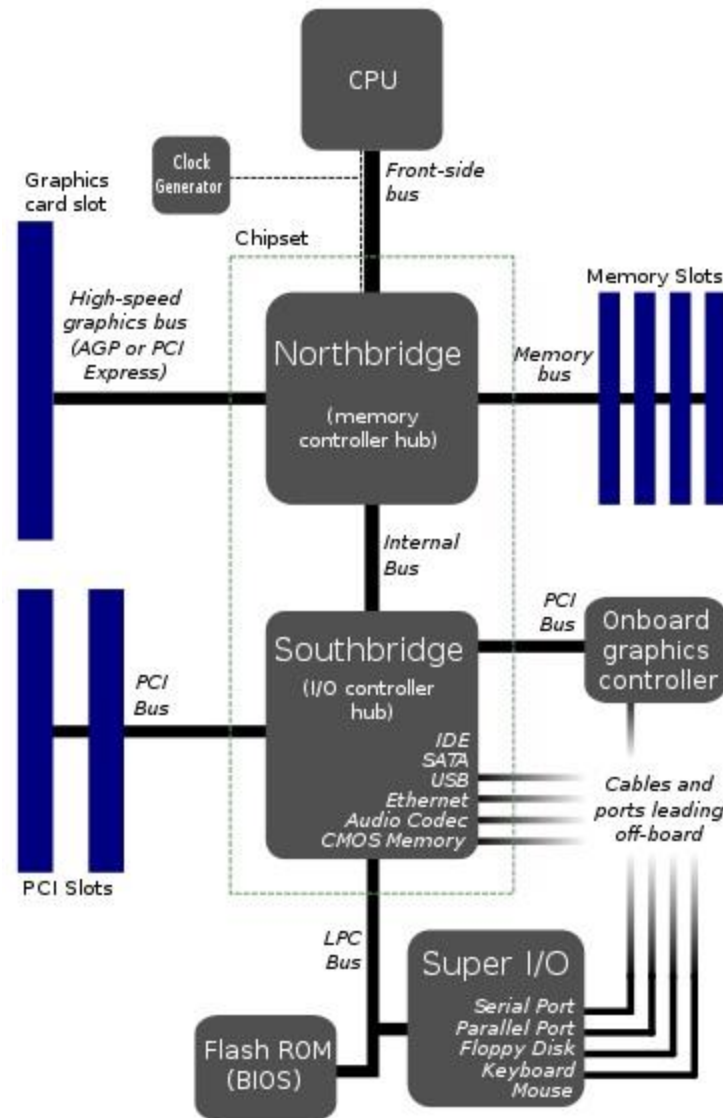
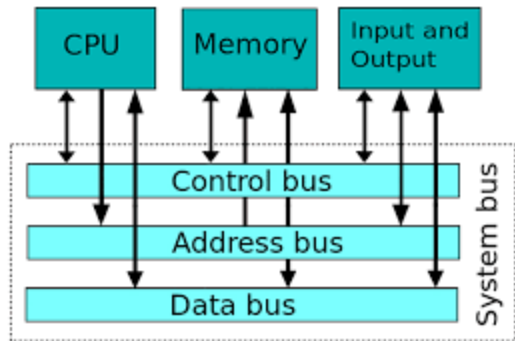
- Tension – When opposite forces (Thrust – the forward force and the Drag – the reverse) apply at the same level – when flying.
- Shear – When the opposite forces work but at different levels (on nuts and bolts of fuselage).
- Compression – When the forces tend to compress an object (during landing is one of the examples)
- Bending - The wings take this stress
- Torsion – Throughout the flight

## An Aircraft movements



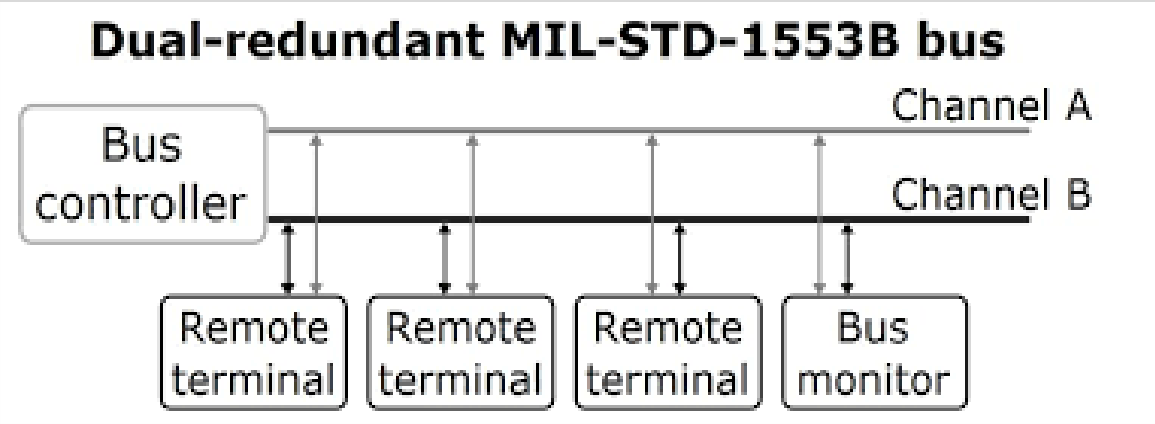
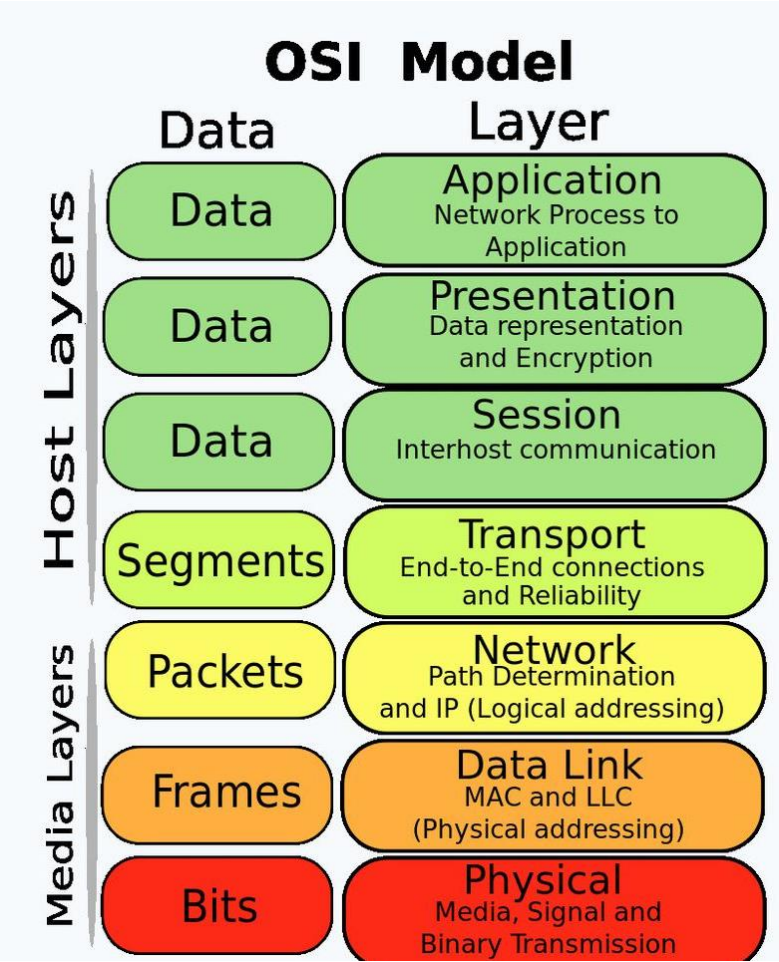


# Concept of Buses



Be clear on the concepts of the below –

- USART / UART
- PCI / PCIe
- RS 232 and RS422 / RS 485
- SPI
- IIC
- USB
- HDMI
- Bluetooth
- CAN/LIN
- MIL 1553
- ARINC 429
- IDE / SCSI



ARINC Bus (high-level)

