Open IMA: Bridging MOSA for Airworthiness Qualification through Civil-Military Functional Safety Management (FSM) Development Assurance (DA) Standards

Dr. Daniel Schrage, Professor Emeritus
Aerospace Systems Design Laboratory
Vertical Lift Research Center of Excellence
School of Aerospace Engineering
Georgia Institute of Technology

Presentation Outline

- What is MOSA and its Systems Engineering & Technical Approach?
- How can Open IMA help MOSA bridge with Civil-Military Functional Safety Management (FSM) and Development Assurance (DA) Standards, for both hardware and software for Airworthiness Qualification, and Certification for Assured Autonomy?
- The Civil-Military FSM and DA Standards accommodate Open IMA, Model Based Systems Engineering (MBSE), Digital Twins & Engineering and Risk Based Assessments for both Civil and Military Aircraft
- The FSM and DA Process can be expanded for Assured Autonomy of Civil and Military Aircraft

What is MOSA?

- ***A Modular Open Systems Approach (MOSA) is an acquisition, modular design, and technical strategy that utilizes open standards for designing an affordable and adaptable system.***
- An open systems design is a **design approach for developing an affordable and adaptable open system**.
- It derives inputs from both the technical management processes and technical processes **undertaken within the systems engineering and other life-cycle processes, and in turn impacts these processes**.
- The open systems design strategy **should be implemented as part of the program's overall technical approach** and becomes an integral part of the program's **Systems Engineering Plan** (SEP) and a summary in their **Acquisition Strategy**.
- The five key elements are identified along with its Authorization, Purpose, Baseline and **Enterprise Architecture Framework (EAF)**

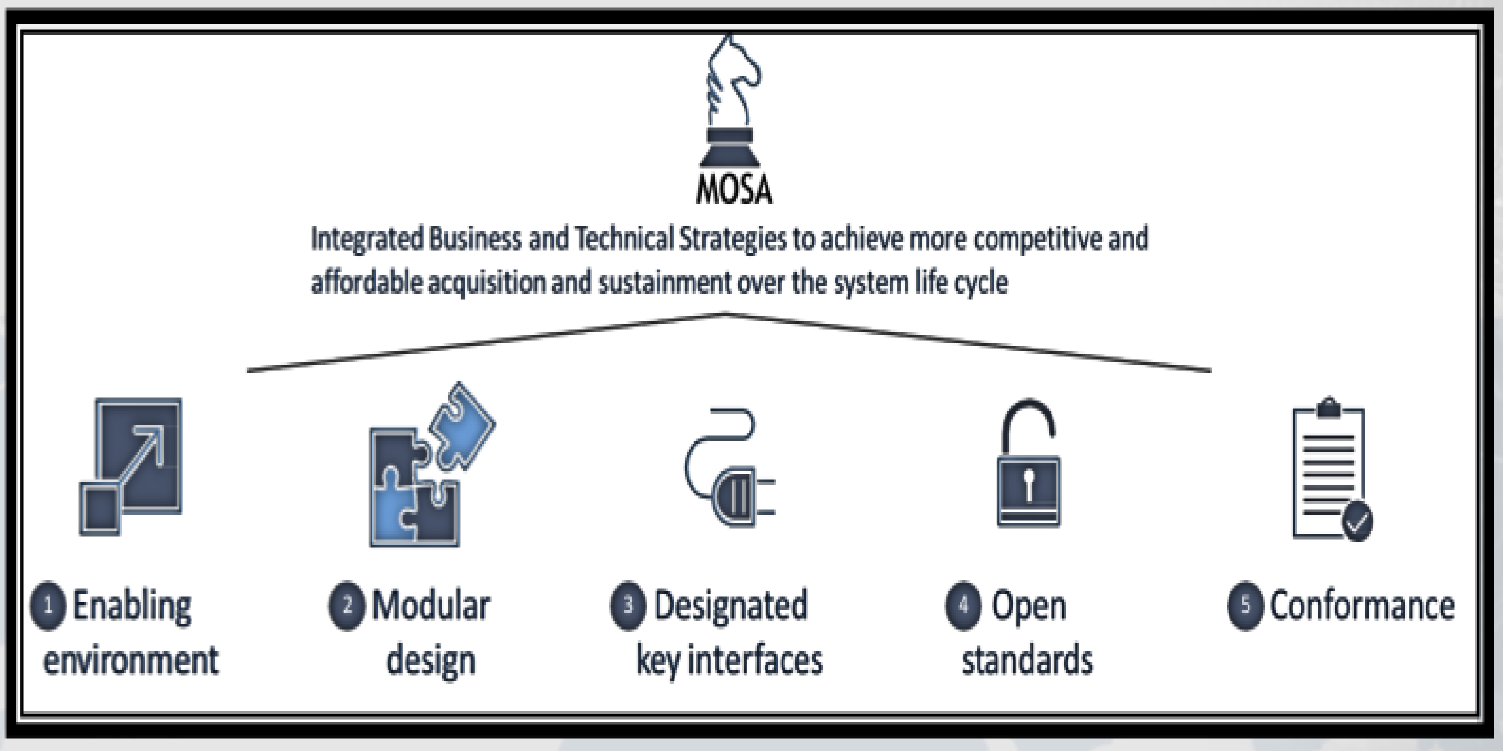
MOSA INNOVATION CHALLENGE

@ Industry and Government Summit & Expo

Atlanta GA 18-19 September 2023
Georgia World Congress Center

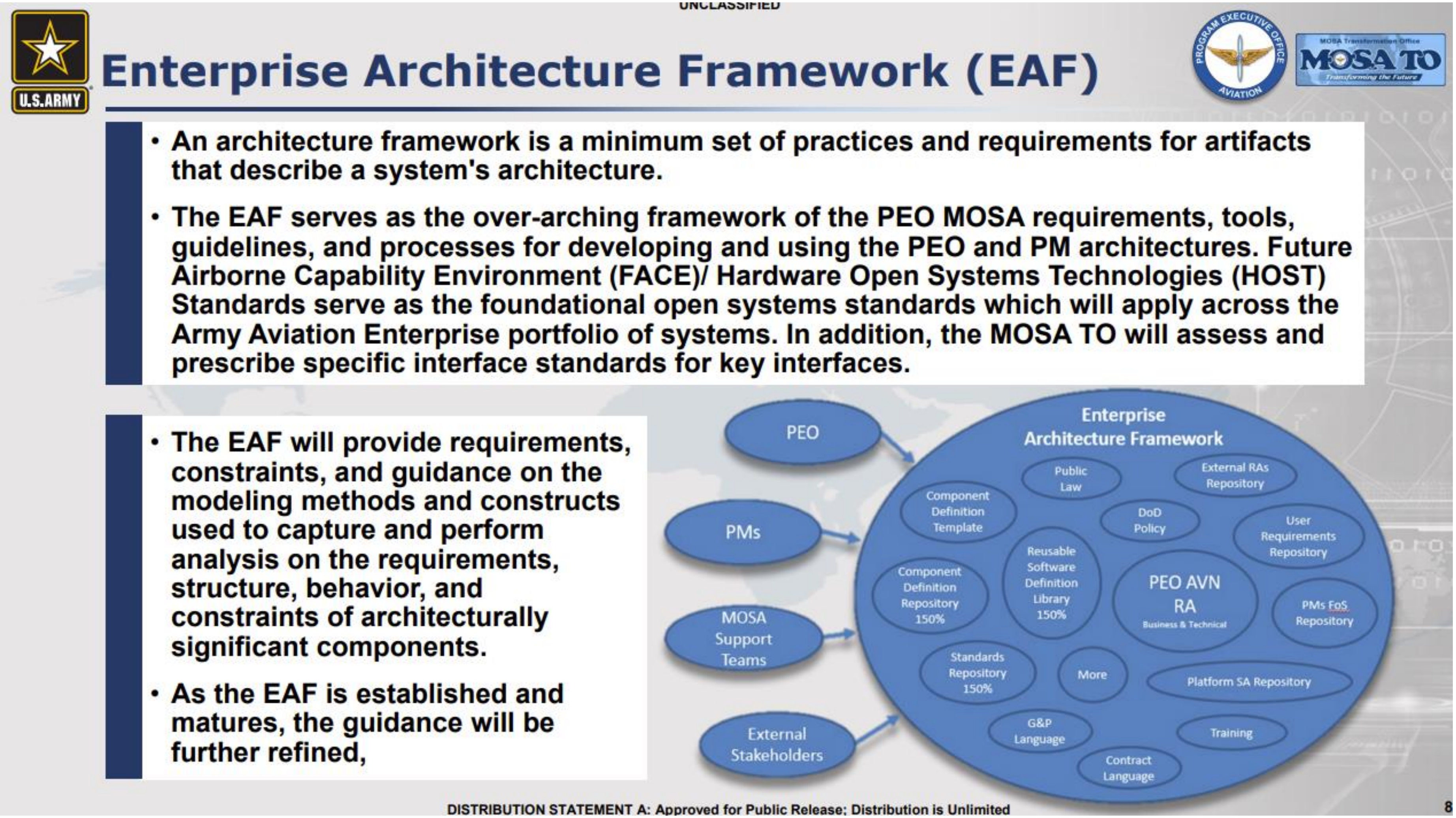
- Twenty-first century air mobility requires 21st century technology: do you have the next-generation communications, computing, or operations technology for enhanced performance, safety and resilience? TechConnect is looking for companies of all sizes interested in collaborating with OEM leaders in the air mobility space
- **Key Major System Components Include:**
  - Aviation Mission Computing Environment (AMCE)
  - Dynamic Airspace & Mission Planning Environment (DAMPE)
  - Airborne Radio Control (ARCM)Aircraft Survivability Equipment (ASE)
  - Common Pilot Vehicle Interface (PVI)
  - Degraded Visual Environment (DVE)
  - Link 16 & C5ISR
  - Navigation
  - Power Distribution
  - Unmanned Vehicle Control
  - MS&T & Readiness

The Army PEO Aviation MOSA Implementation Guide has Five Key Elements


MOSA
Integrated Business and Technical Strategies to achieve more competitive and affordable acquisition and sustainment over the system life cycle
1 Enabling environment
2 Modular design
3 Designated key interfaces
4 Open standards
5 Conformance

However, A Systems Engineering Process for Aircraft Development, Safety Assessment, Certification and Airworthiness Qualification needs to be bridged for Functional and Physical Avionics Architectures using Open IMA which has not been addressed as a Means of Compliance (MOC) in the Army Military Airworthiness Certification Criteria (AMACC), 2019 or its Changes 1&2, 2021 and 2023

PEO Aviation Enterprise Architecture Framework (EAF)



UNCLASSIFIED

U.S.ARMY

Enterprise Architecture Framework (EAF)

PROGRAM EXECUTIVE OFFICE AVIATION

MOSA Transformation Office MOSA TO *Transforming the Future*

- An architecture framework is a minimum set of practices and requirements for artifacts that describe a system's architecture.
- The EAF serves as the over-arching framework of the PEO MOSA requirements, tools, guidelines, and processes for developing and using the PEO and PM architectures. Future Airborne Capability Environment (FACE)/ Hardware Open Systems Technologies (HOST) Standards serve as the foundational open systems standards which will apply across the Army Aviation Enterprise portfolio of systems. In addition, the MOSA TO will assess and prescribe specific interface standards for key interfaces.

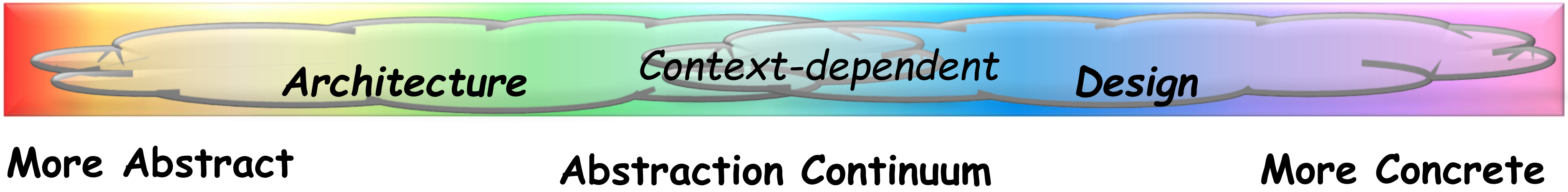
- The EAF will provide requirements, constraints, and guidance on the modeling methods and constructs used to capture and perform analysis on the requirements, structure, behavior, and constraints of architecturally significant components.
- As the EAF is established and matures, the guidance will be further refined,

DISTRIBUTION STATEMENT A: Approved for Public Release; Distribution is Unlimited

8

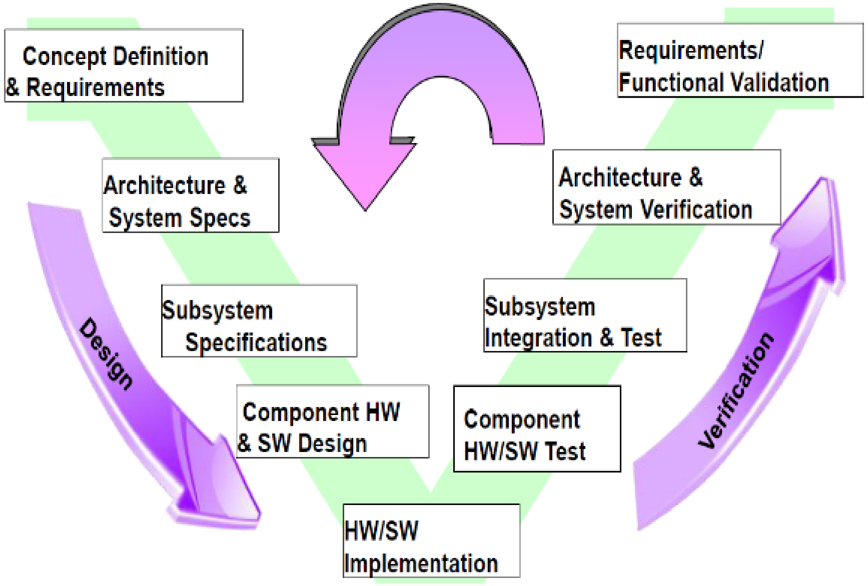
Understanding Architectures: From SOS to System to Physical to Desgin

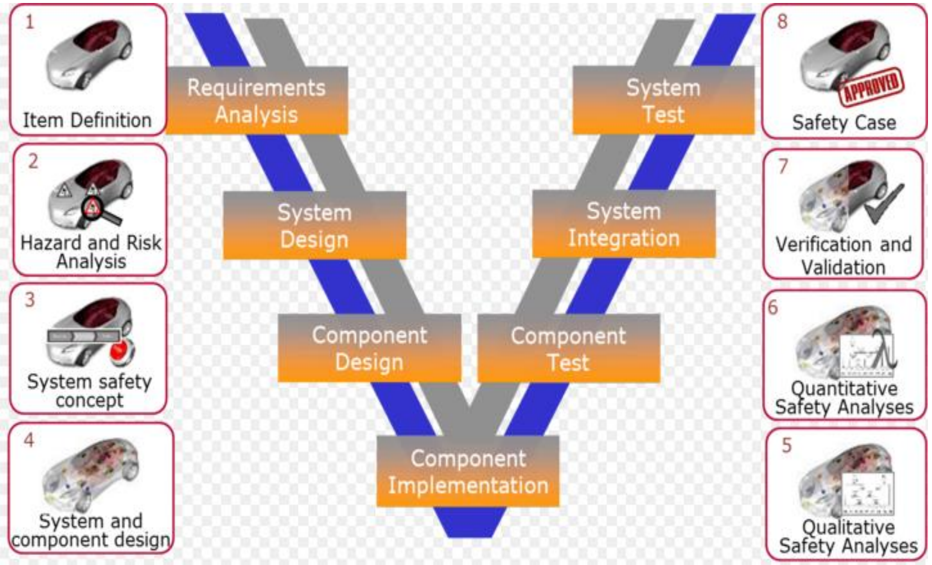
- **Most agree that there’s a difference between architecture and design**
  - **Both talk about specification, but to different degrees**: **a detailed Architecture specification can be implemented in more than one way, but a detailed design can’t**.
    - A design (that complies with the Architecture) is therefore required to proceed to implementation



  - **Architecture applies analysis along dimensions that Design usually does not:**
    - organizational/technical/legal risks, impacts and dependencies
    - future-state projections (transitional solutions, roadmaps),
    - deviations from Strategy or standards
    - solution qualities (scalability, reliability, …)
    - etc.
  - **Architecture addresses alignment, construction, deployment, operational and retirement aspects of a solution; Design often is just about construction and execution**

Simplified Vee Diagram Views of Transition from Architecture to Design


Concept Definition & Requirements
Architecture & System Specs
Subsystem Specifications
Component HW & SW Design
HW/SW Implementation
Component HW/SW Test
Subsystem Integration & Test
Architecture & System Verification
Requirements/ Functional Validation
Design
Verification

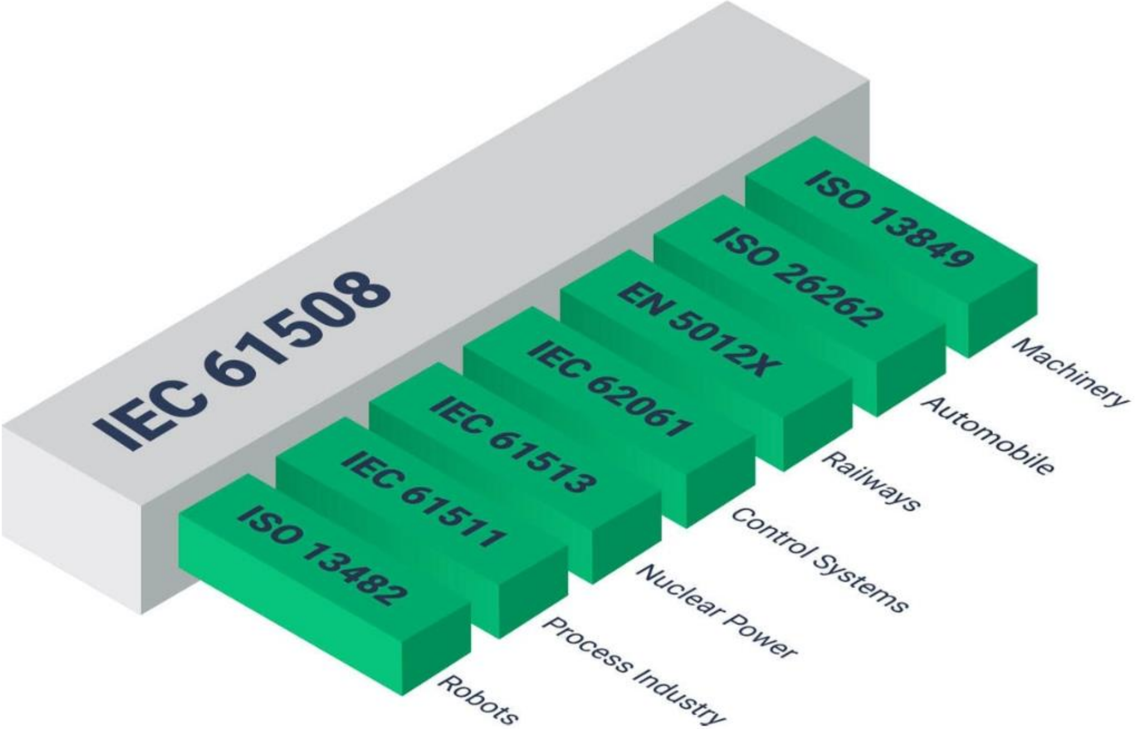


Architecture to Design to Implementation Focus **An Automotive Example w/o Architecture**

ISO 61508 Standard Development Assurance (DA) Approach Now included in Numerous Other Standards

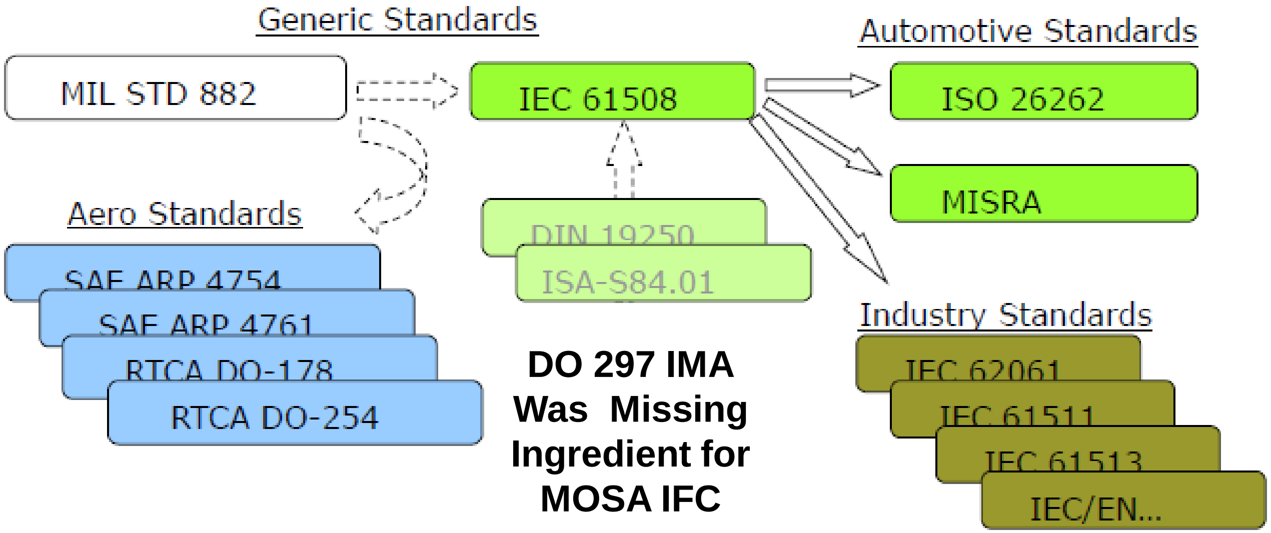
(DA Standards Integrated W/Design Time Assurance (DTA) & Run Time Assurance (RTA
Are Required for Assured Autonomy of Future Aviation Systems)

- These functional safety standards deliver benefits to developers, system integrators and users.
- By following a standard, a development organization builds safer products.
- A system integrator can state its expectations to a supplier by requiring compliance with a standard users have fewer injuries and deaths.



Evolution of Standards, Not Just Software

- MIL STD-882 *System Safety* is an overall Military Standard, but the Military has no equivalent *Aircraft Development Assurance Standard*.
- Military has to accept DO178 for Software and DO254 for Electric HW



Generic Standards

MIL STD 882

IEC 61508

DIN 19250

ISA-S84.01

Automotive Standards

ISO 26262

MISRA

Aero Standards

SAE ARP 4754

SAE ARP 4761

RTCA DO-178

RTCA DO-254

Industry Standards

IEC 62061

IEC 61511

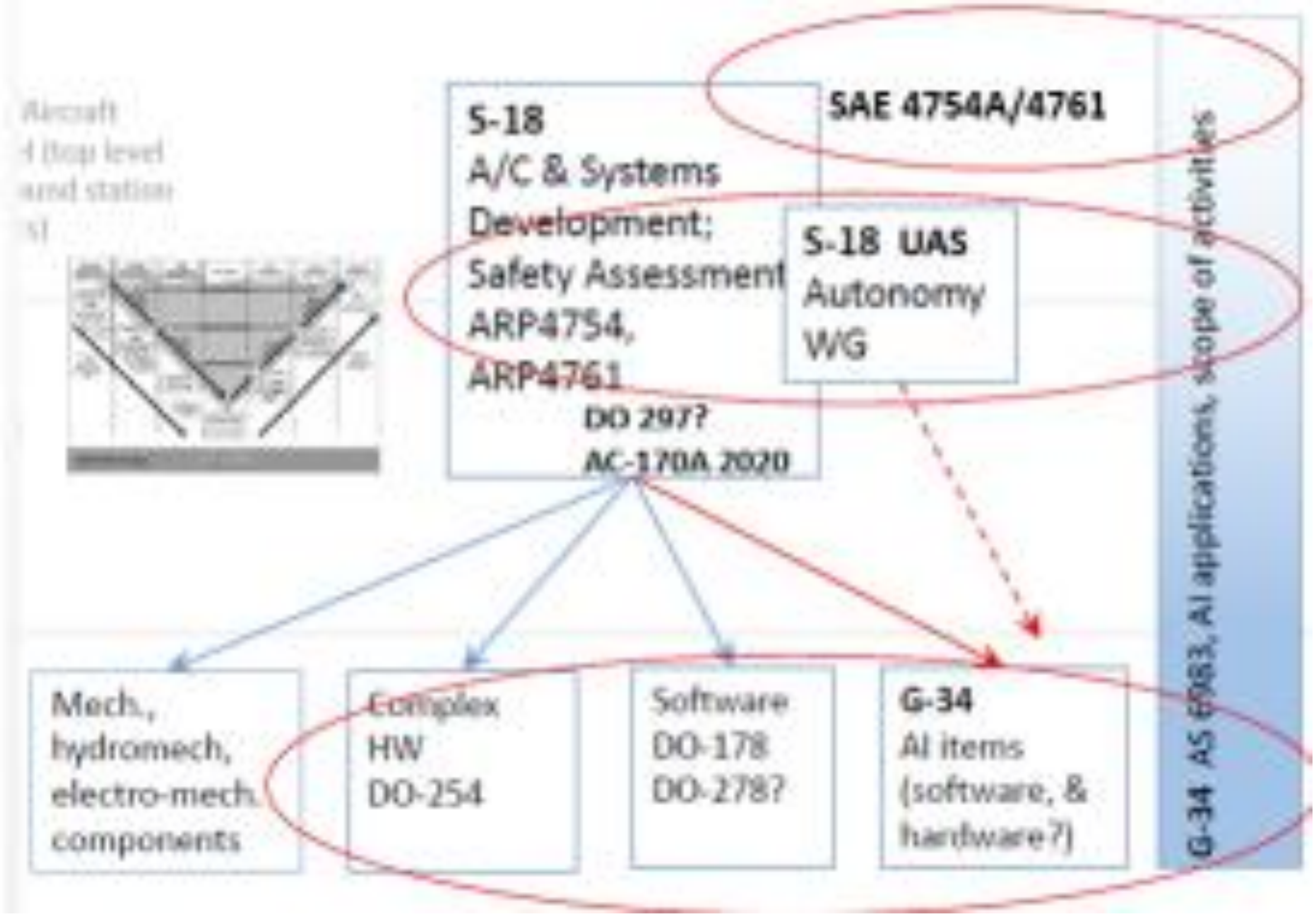
IEC 61513

IEC/EN...

DO 297 IMA Was Missing Ingredient for MOSA IFC

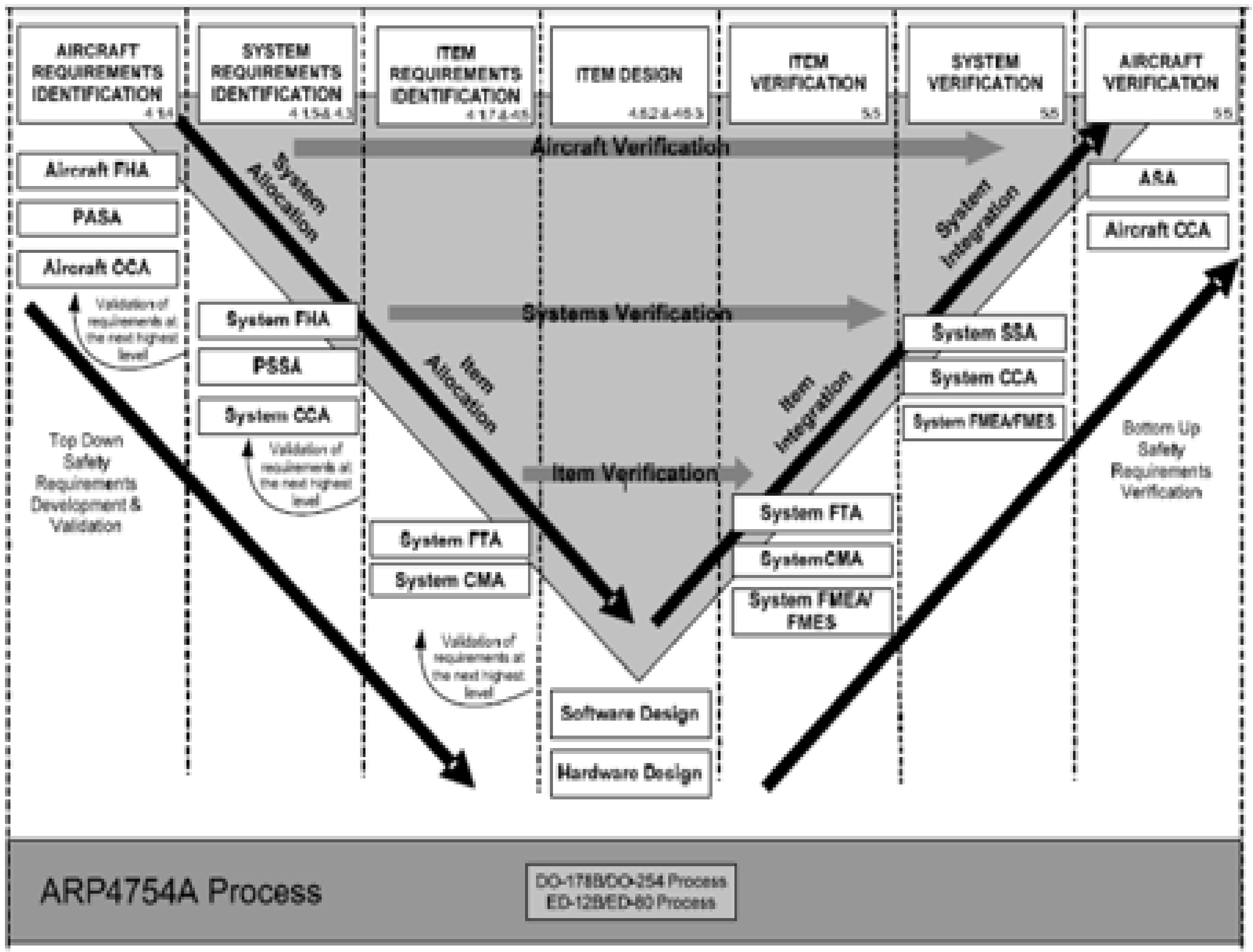
- Recently, 2019, Army Aviation has accepted ARP4754A/4761 as a MOC in Army Military Airworthiness Certification Critieria (AMACC); however, Increase use of Multi-Core Processors (MCPs) requires the need for including DO297 Open IMA for FVL and beyond Certification
- In the last ten years the Military Services have introduced MIL-HDBK 516: *Airworthiness Certification* as a catchall for all AW requirements, but no IMA

SAE 18 Working Group on Autonomy and G34 Standard on AI has been active last few years (I have served as a Member)



The SAE ARP 4754A and 4761 Civil-Military FSM and DA Standards provide the Aircraft Systems Engineering Development & Safety Assessment Vee Diagram used successfully for Certification throughout the World

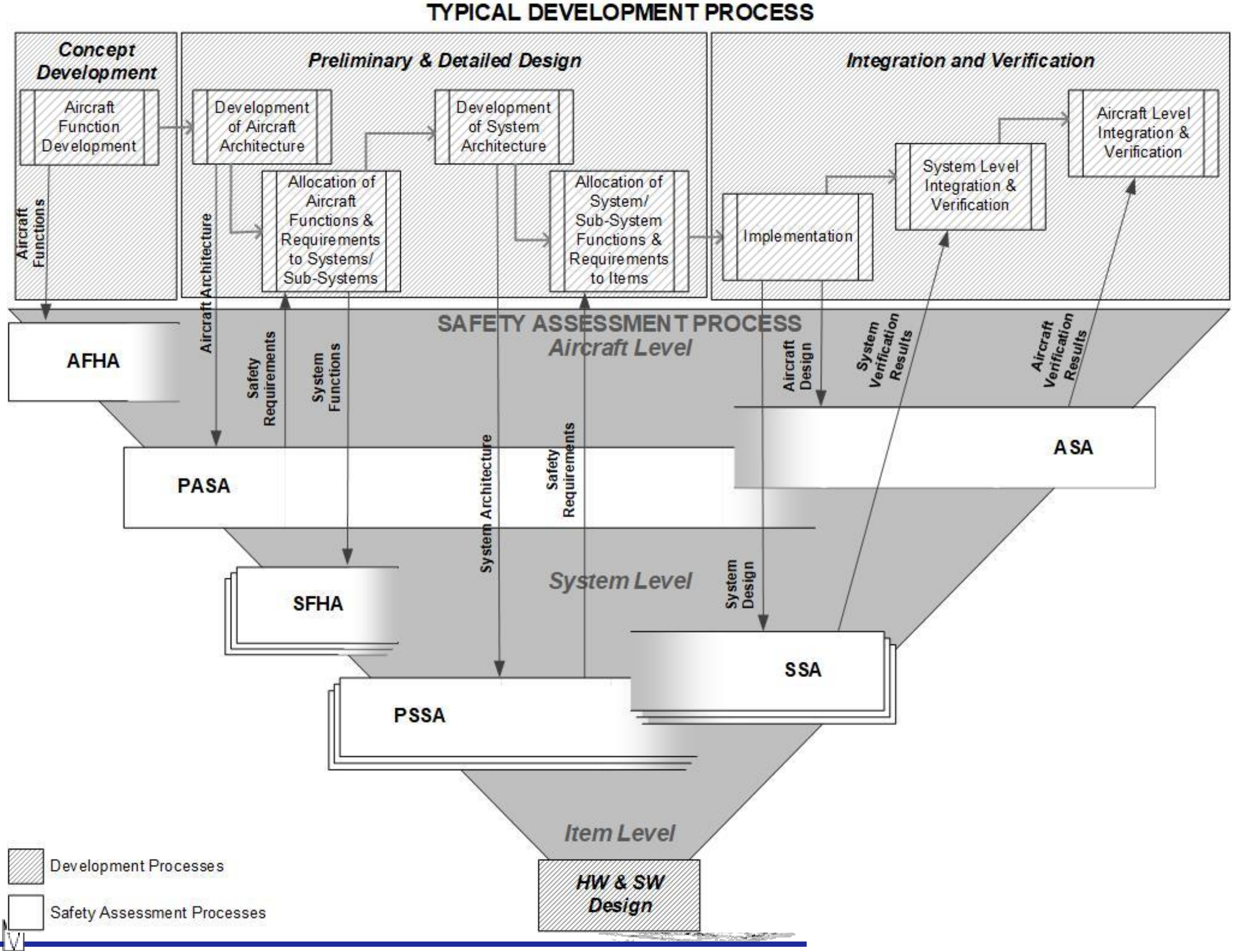
DEVELOPMENT ASSURANCE (DA)



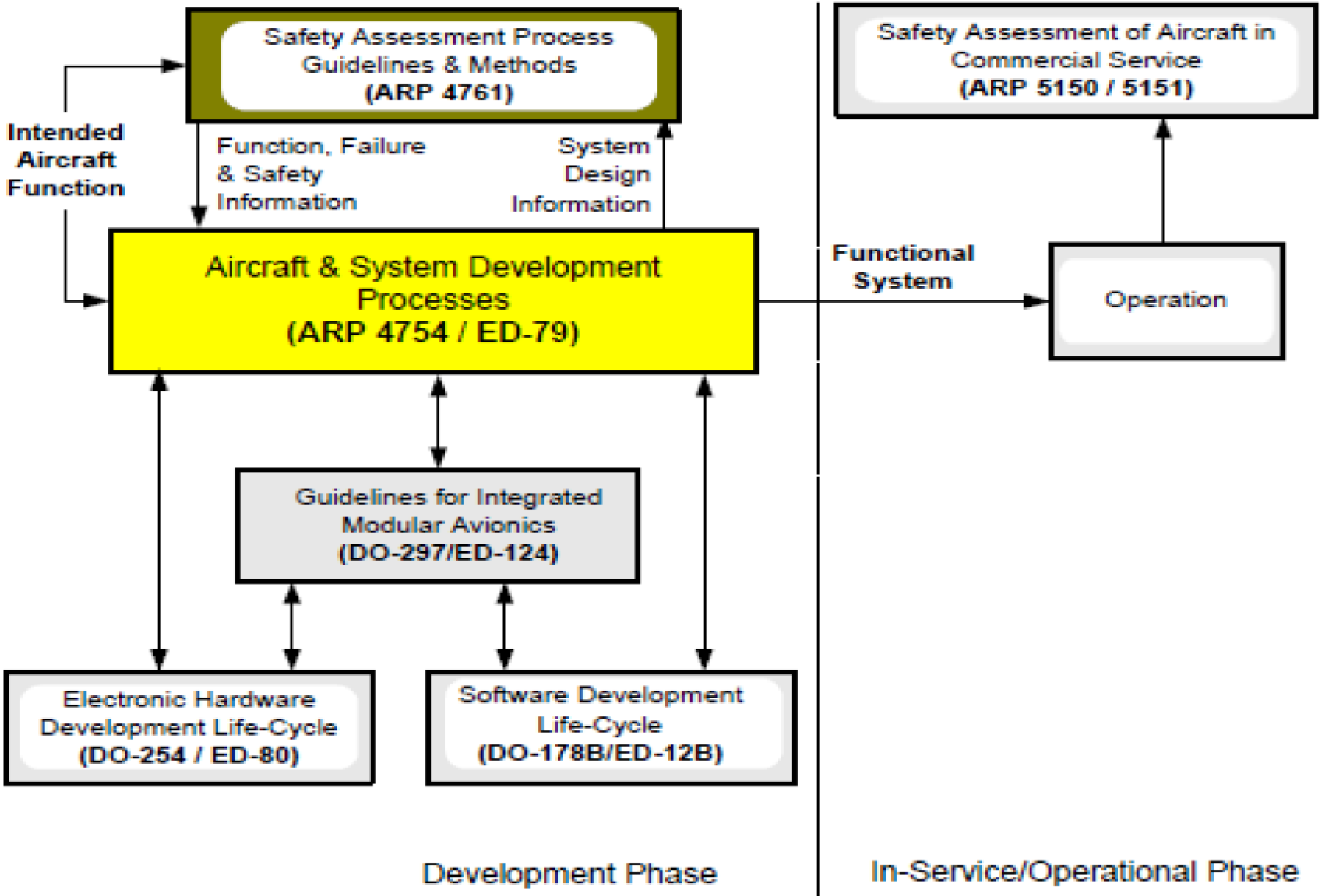
QUALIFICATION ASSURANCE (QA)

Civil Aircraft Focus on Development Assurance; Military Aircraft on Qualification Assurance

Integrated Aircraft & Systems Development and Safety Assessment Processes for Hardware & Software Design

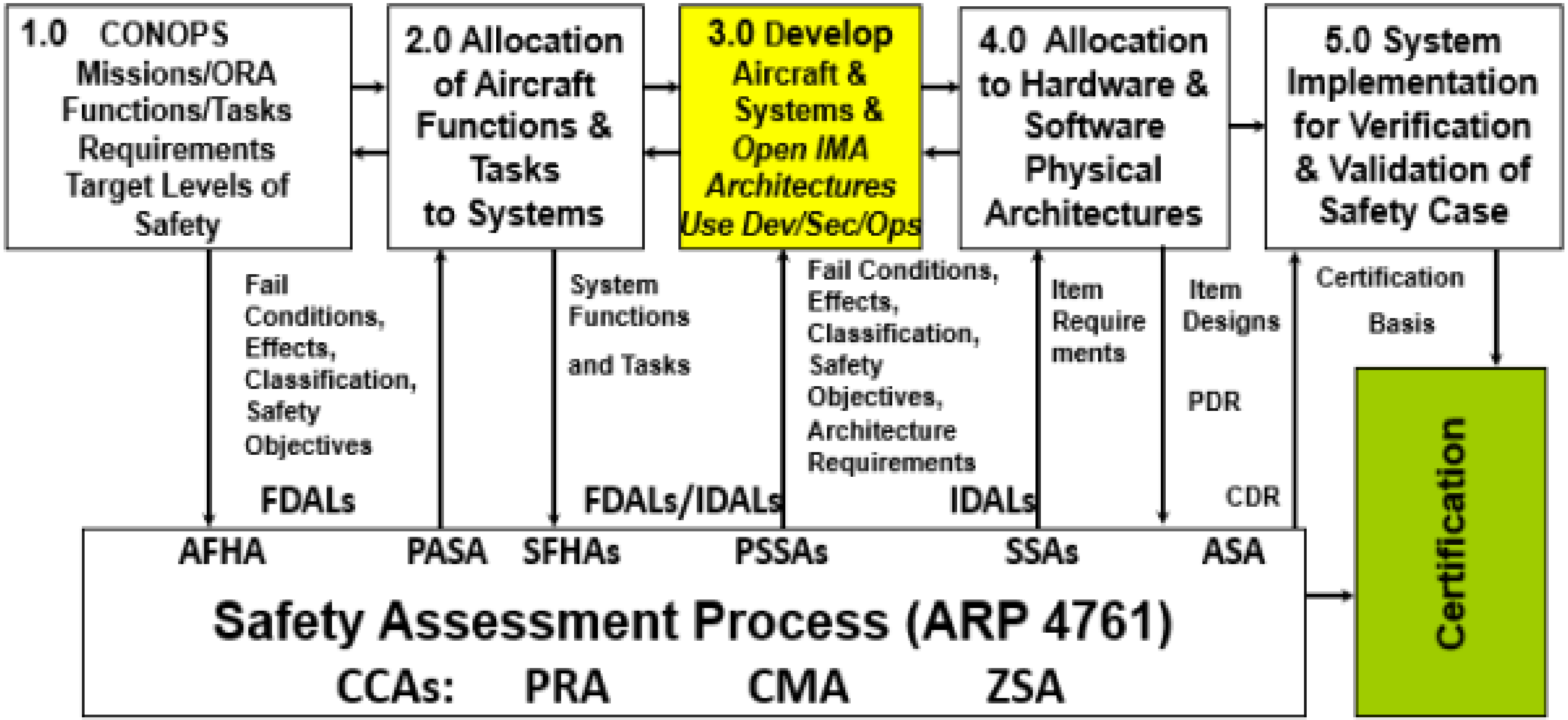

TYPICAL DEVELOPMENT PROCESS
Concept Development
Preliminary & Detailed Design
Integration and Verification
Aircraft Function Development
Development of Aircraft Architecture
Allocation of Aircraft Functions & Requirements to Systems/ Sub-Systems
Development of System Architecture
Allocation of System/ Sub-System Functions & Requirements to Items
Implementation
System Level Integration & Verification
Aircraft Level Integration & Verification
Aircraft Functions
Aircraft Architecture
Safety Requirements
System Functions
System Architecture
Safety Requirements
Aircraft Design
System Verification Results
Aircraft Verification Results
System Design
SAFETY ASSESSMENT PROCESS
Aircraft Level
AFHA
PASA
ASA
System Level
SFHA
PSSA
SSA
Item Level
HW & SW Design
Development Processes
Safety Assessment Processes

The 2010 Issuance of ARP 4754A/ED-79 provided a Global Functional Safety Standard, included component hardware, software and Integrated Modular Avionics (IMA) for Aircraft Synthesis



A Civil-Military Functional Safety Management (FSM) Development Assurance (DA) Open IMA Framework for Assured Autonomy for Air Vehicles is Required

Civil & Military Aircraft & Systems Development Process (ARP 4754A)

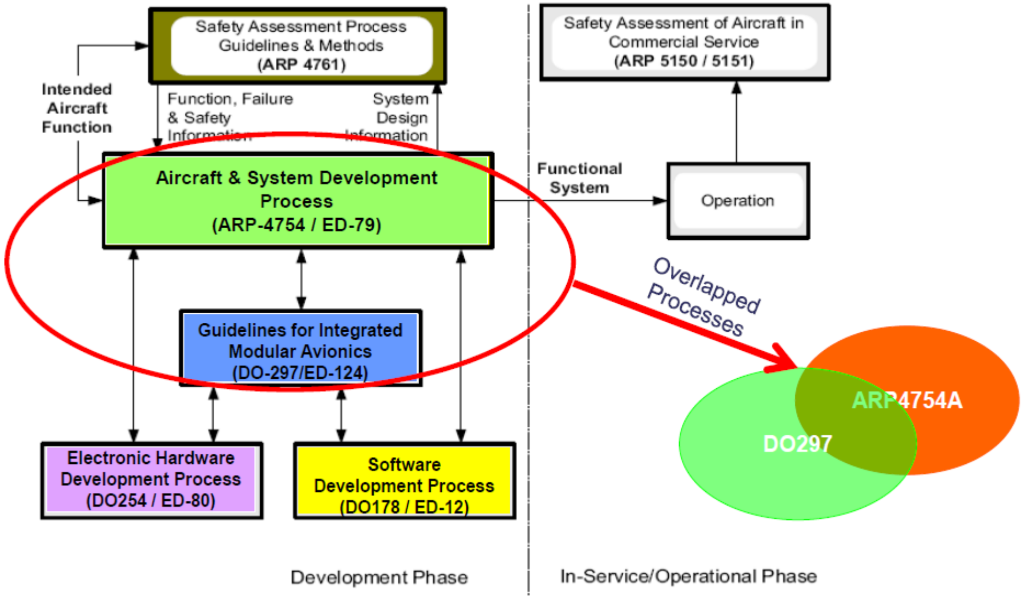

1.0 CONOPS Missions/ORA Functions/Tasks Requirements Target Levels of Safety
2.0 Allocation of Aircraft Functions & Tasks to Systems
3.0 Develop Aircraft & Systems & Open IMA Architectures Use Dev/Sec/Ops
4.0 Allocation to Hardware & Software Physical Architectures
5.0 System Implementation for Verification & Validation of Safety Case
Fail Conditions, Effects, Classification, Safety Objectives
FDALs
System Functions and Tasks
FDALs/IDALs
Fail Conditions, Effects, Classification, Safety Objectives, Architecture Requirements
IDALs
Item Require ments
Item Designs
PDR
CDR
Certification Basis
AFHA
PASA
SFHAs
PSSAs
SSAs
ASA
Safety Assessment Process (ARP 4761)
CCAs: PRA CMA ZSA
Certification

Aircraft/System/Hardware/Software Industrial Standards for Open Integrated Modular Avionics (IMA) will be the Key for Assured Autonomy for Autonomous Air Vehicles

- **DO 297 (2005), IMA Development Guidance & Certification** Considerations and ARP4754A (2010), need close coupling for autonomous air vehicles

- **Open IMA** also Interacts with the followings standards
  - ARP 4761, Safety Assessment
  - DO 254, Electronic Hardware
  - DO 178C, Software Certification
  - ARINC 653 Avionics Application Standard Software Interface, RTOS
  - ARINC 664 Avionics Interfaces
- **Multi-Core Processors for Assured Autonomy** requires these standards plus the closer coupling of ARP 4754B & DO297

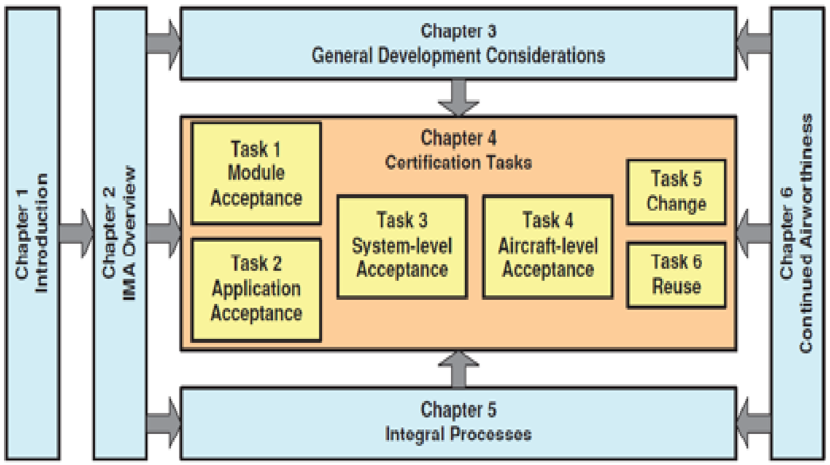
- **Civil Aviation has moved to Open IMA** and a closer coupling of ARP 4754A & DO297

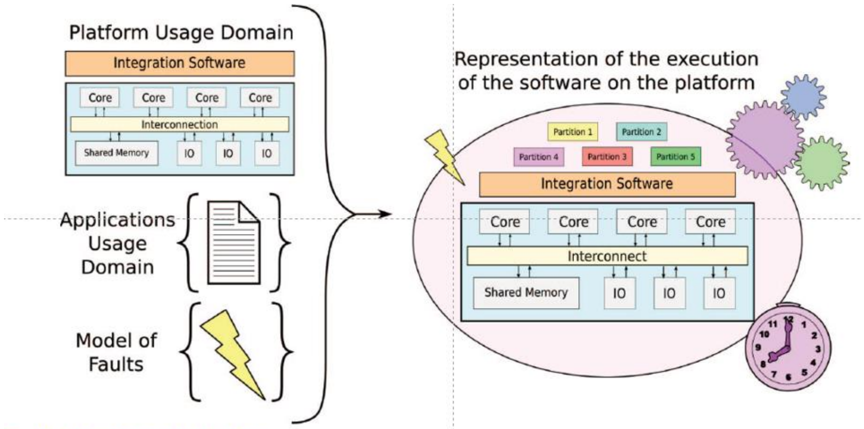


Safety Assessment Process Guidelines & Methods (ARP 4761)
Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)
Intended Aircraft Function
Function, Failure & Safety Information
System Design Information
Aircraft & System Development Process (ARP-4754 / ED-79)
Functional System
Operation
Overlapped Processes
Guidelines for Integrated Modular Avionics (DO-297/ED-124)
ARP4754A
DO297
Electronic Hardware Development Process (DO254 / ED-80)
Software Development Process (DO178 / ED-12)
Development Phase
In-Service/Operational Phase

- **Military Aviation must move to Open IMA**& a closer coupling of ARP 4754 & DO297 for **Assured Autonomy**

DO 297 IMA Tasks, Stakeholders and Implementation on ARINC 653 with Multi-Core Processors and Mandatory Requirements

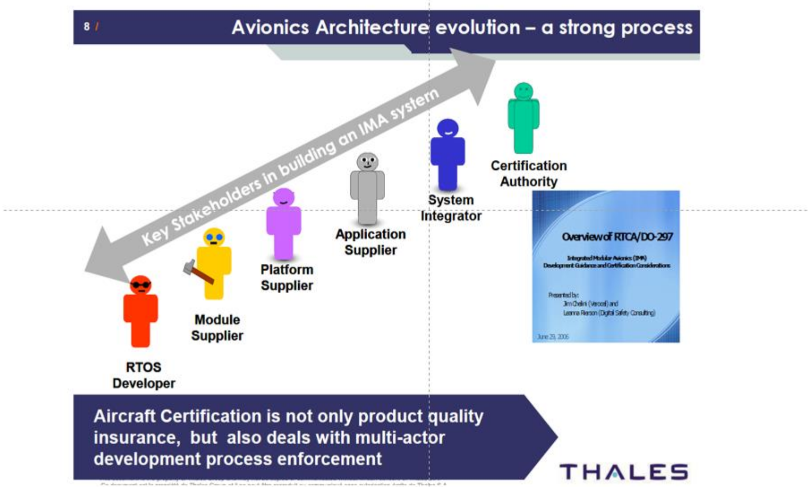




- Robust partitioning
- Platform determinism
- Platform limitations for WCET scenario definition

IMA Certification Requires Collaboration Between A Number of Stakeholders

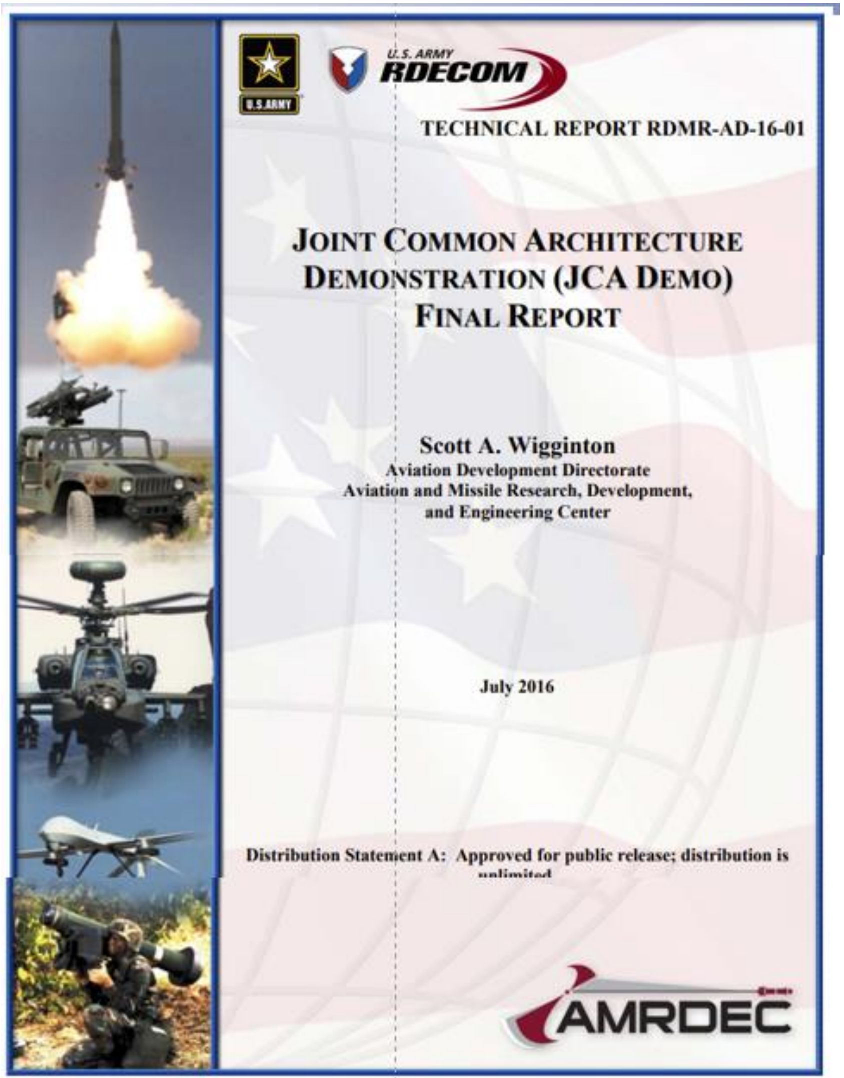
(Gatti, M. International Conference on Integrated Modular Avionics – MoscowThe EC FP7 R&D project: *SCARLETT*, 2012-10-29)


8 / Avionics Architecture evolution – a strong process

Aircraft Certification is not only product quality insurance, but also deals with multi-actor development process enforcement

- **Hardware/Software Integration**—The process of combining software into the target computer.
- **IMA System Integrator**—The developer who performs the activities necessary to integrate the platform(s), modules, and components with the hosted applications to produce the IMA system.
- **RTOS Supplier**—The RTOS supplier, as a member of the platform and module supplier role, has critical responsibilities of protectionwith regards to space, time, I/O, and other shared resources on the IMA system

The Joint Common Architecture Demonstration (JCA Demo) project was the first in a series of planned experiments under the Joint Multi-Role (JMR) Technology Demonstrator (TD) Mission Systems Architecture Demonstration (MSAD) Science and Technology (S&T) effort, July 2016



U.S. ARMY

U.S. ARMY RDECOM

TECHNICAL REPORT RDMR-AD-16-01

JOINT COMMON ARCHITECTURE DEMONSTRATION (JCA DEMO) FINAL REPORT

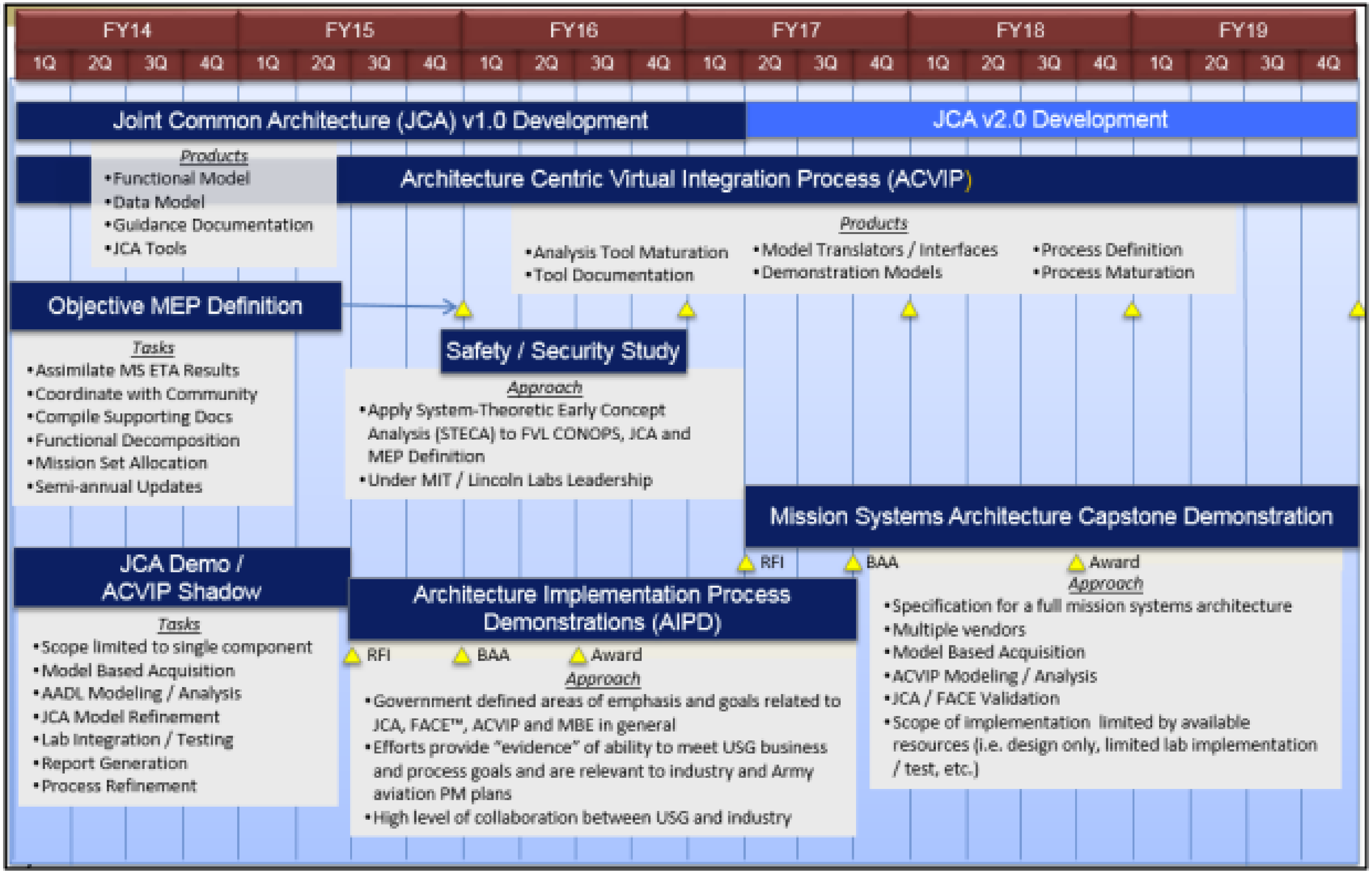
Scott A. Wigginton
Aviation Development Directorate
Aviation and Missile Research, Development,
and Engineering Center

July 2016

Distribution Statement A: Approved for public release; distribution is unlimited

AMRDEC

Joint Common Architecture (JCA) Development



FY14				FY15				FY16				FY17				FY18				FY19			
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q

Joint Common Architecture (JCA) v1.0 Development

JCA v2.0 Development

Products
- Functional Model
- Data Model
- Guidance Documentation
- JCA Tools

Architecture Centric Virtual Integration Process (ACVIP)

Products
- Analysis Tool Maturation
- Tool Documentation
- Model Translators / Interfaces
- Demonstration Models
- Process Definition
- Process Maturation

Objective MEP Definition

Tasks
- Assimilate MS ETA Results
- Coordinate with Community
- Compile Supporting Docs
- Functional Decomposition
- Mission Set Allocation
- Semi-annual Updates

Safety / Security Study

Approach
- Apply System-Theoretic Early Concept Analysis (STECA) to FVL CONOPS, JCA and MEP Definition
- Under MIT / Lincoln Labs Leadership

Mission Systems Architecture Capstone Demonstration

RFI BAA Award

Approach
- Specification for a full mission systems architecture
- Multiple vendors
- Model Based Acquisition
- ACVIP Modeling / Analysis
- JCA / FACE Validation
- Scope of implementation limited by available resources (i.e. design only, limited lab implementation / test, etc.)

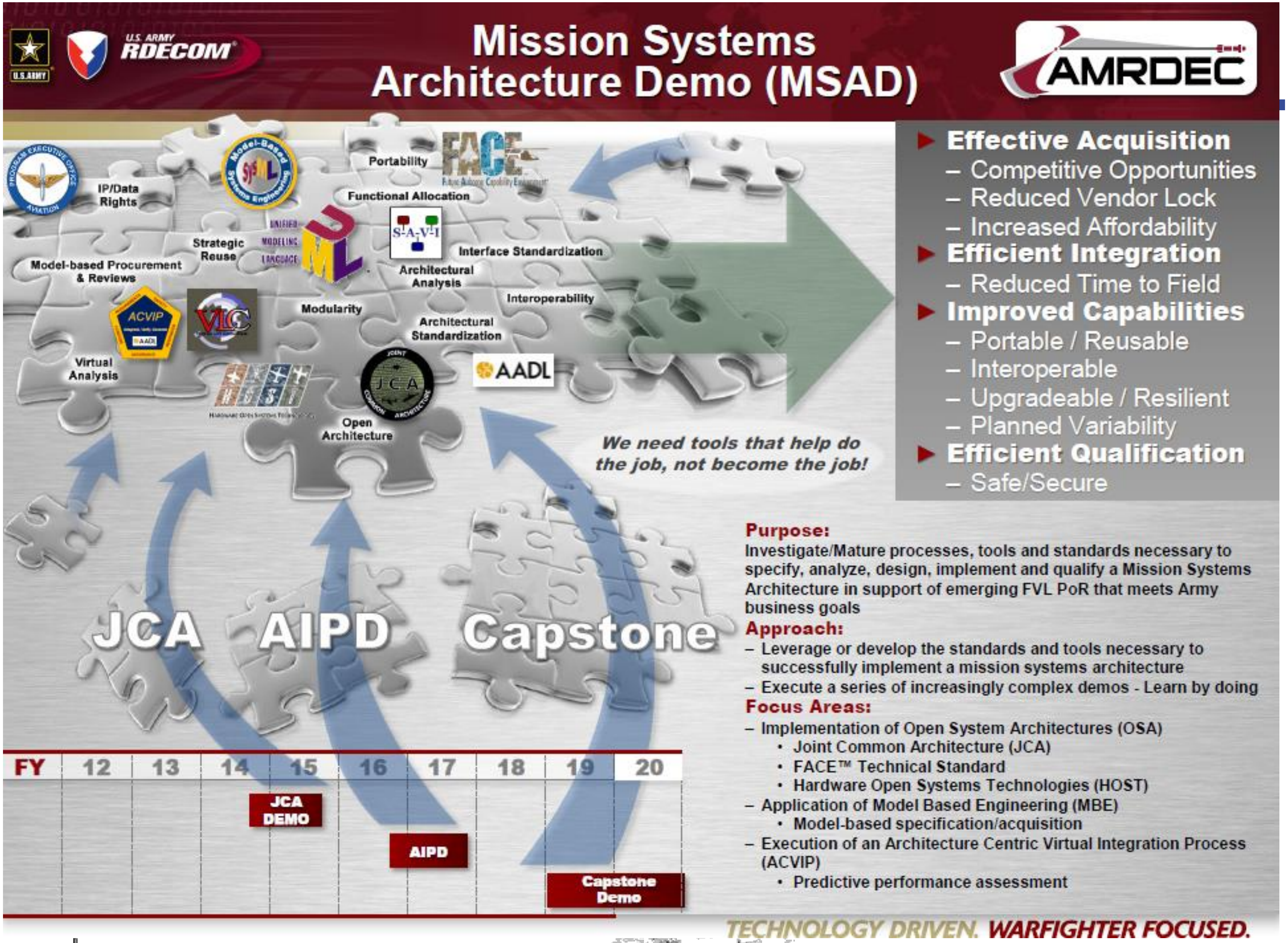
JCA Demo / ACVIP Shadow

Tasks
- Scope limited to single component
- Model Based Acquisition
- AADL Modeling / Analysis
- JCA Model Refinement
- Lab Integration / Testing
- Report Generation
- Process Refinement

Architecture Implementation Process Demonstrations (AIPD)

RFI BAA Award

Approach
- Government defined areas of emphasis and goals related to JCA, FACE™, ACVIP and MBE in general
- Efforts provide "evidence" of ability to meet USG business and process goals and are relevant to industry and Army aviation PM plans
- High level of collaboration between USG and industry



Mission Systems Architecture Demo (MSAD)

- **Effective Acquisition**
  - Competitive Opportunities
  - Reduced Vendor Lock
  - Increased Affordability
- **Efficient Integration**
  - Reduced Time to Field
- **Improved Capabilities**
  - Portable / Reusable
  - Interoperable
  - Upgradeable / Resilient
  - Planned Variability
- **Efficient Qualification**
  - Safe/Secure

We need tools that help do the job, not become the job!

Purpose:

Investigate/Mature processes, tools and standards necessary to specify, analyze, design, implement and qualify a Mission Systems Architecture in support of emerging FVL PoR that meets Army business goals

Approach:

- Leverage or develop the standards and tools necessary to successfully implement a mission systems architecture
- Execute a series of increasingly complex demos - Learn by doing

Focus Areas:

- Implementation of Open System Architectures (OSA)
  - Joint Common Architecture (JCA)
  - FACE™ Technical Standard
  - Hardware Open Systems Technologies (HOST)
- Application of Model Based Engineering (MBE)
  - Model-based specification/acquisition
- Execution of an Architecture Centric Virtual Integration Process (ACVIP)
  - Predictive performance assessment

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Joint Common Architecture (JCA) Demonstration Architecture Centric Virtual Integration Process (ACVIP) Shadow Effort

(Boydston, A, Feiler,P, Vestal, S. & Lewis, B., "Presented at the AHS 71st Annual Forum, Virginia Beach, Virginia, May 5, 2015")

- Challenging problems associated with system software complexity growth are threatening industry's ability to build next generation safety critical embedded systems including helicopter avionics systems. Leading to Open Integrated Modular Avionics (IMA)
- Contributors to these problems include the growth of software, system integration, and interaction complexity exacerbated by ambiguous, missing, incomplete, and inconsistent requirements.
- Problems continue to hamper systems in the areas of resource utilization, timing, safety and security.
- A new approach called Architecture Centric Virtual Integration Process (ACVIP) was based on the Society of Automotive Engineers (SAE) Standard AS5506A Architecture Analysis and Design Language (AADL) was being developed and investigated by the US Army to address these challenges.

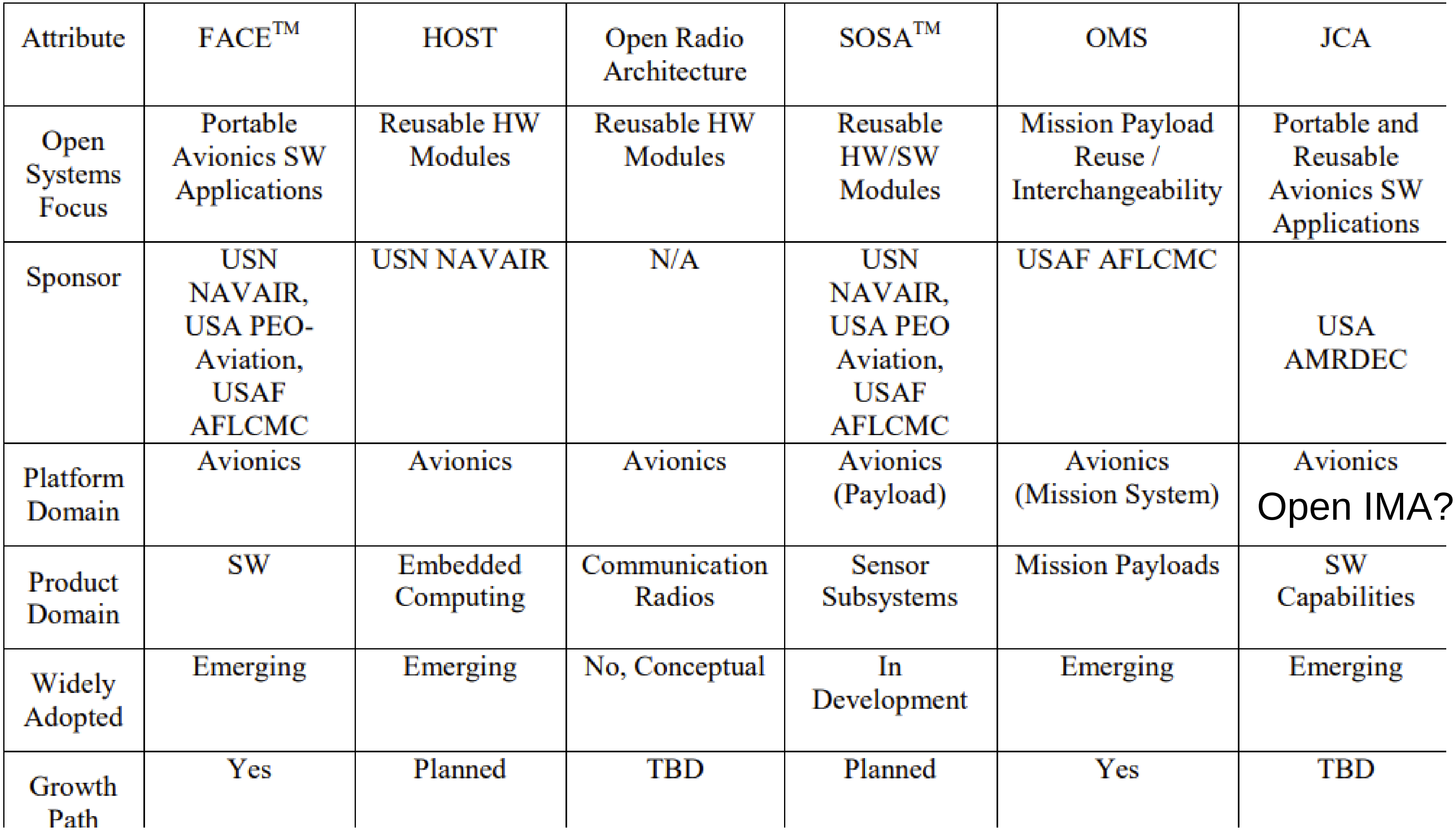
Joint Common Architecture (JCA) Demonstration Architecture with Centric Virtual Integration Process (ACVIP) Shadow Effort

(Boydston, A, Feiler,P, Vestal, S. & Lewis, B., “Presented at the AHS 71st Annual Forum, Virginia Beach, Virginia, May 5, 2015”)

- Problems continue to hamper systems in the areas of resource utilization, timing, safety and security.
- ACVIP is a quantitative, architecture-centric, model-based approach enabling virtual integration analysis in the early phases and throughout the lifecycle to detect and remove defects that currently are not found until software and systems integration and acceptance testing.
- In an effort to investigate such an approach, the Government, in conjunction with researchers from Carnegie Mellon University (CMU) Software Engineering Institute® (SEI) and Adventium Labs®, are conducting ACVIP requirements, safety, and timing analyses **in parallel with the Joint Common Architecture (JCA) Demonstration (Demo)**
- **Was quickly abandoned when FVL moved to Futures Command**

Key Open Architecture Standard Attributes

(Shepherd, K. and Jeremy Wills, J., “Avionics Open Systems Architecture Standardization”, AHS 74th Forum, 2018)

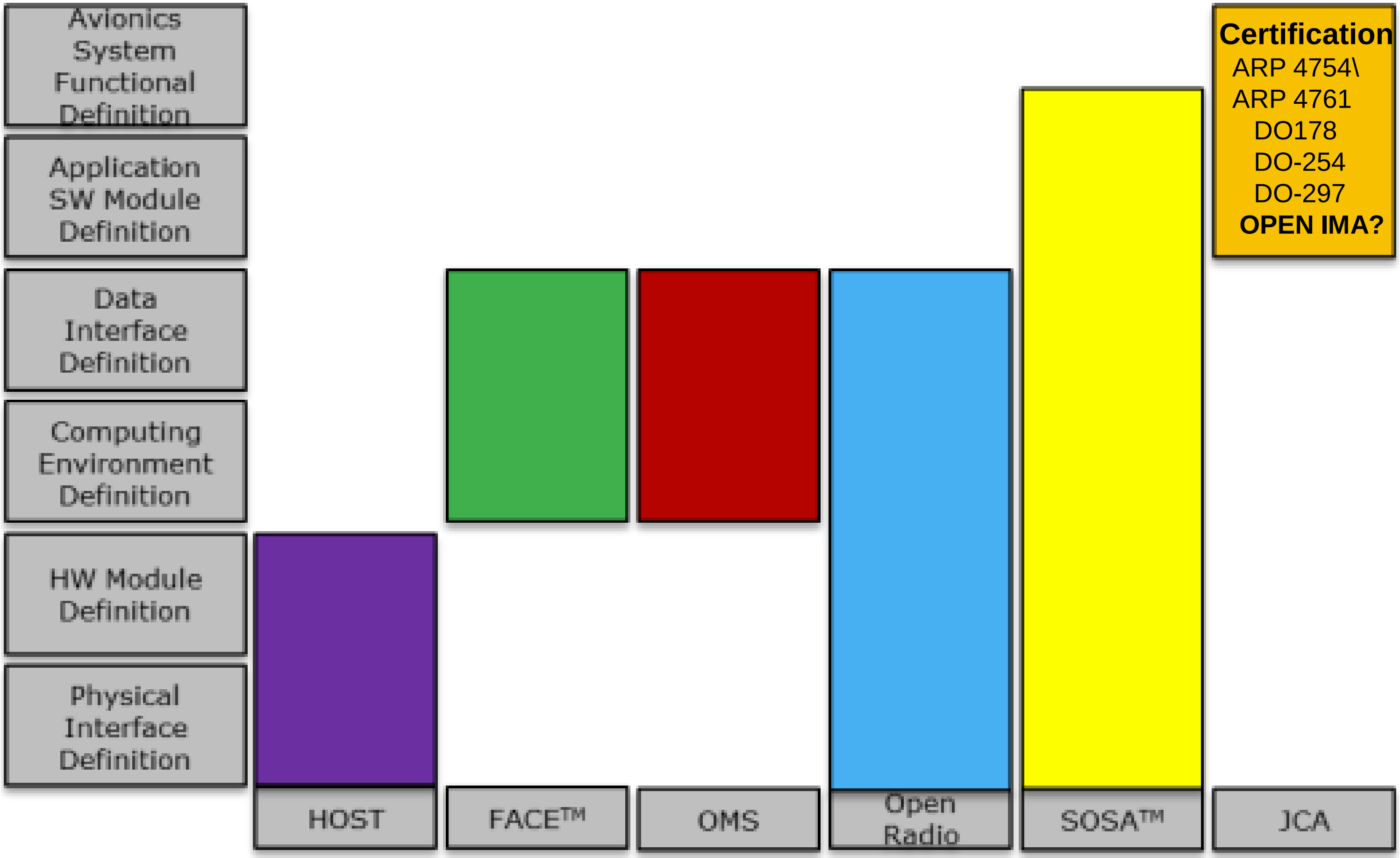


Attribute	FACE™	HOST	Open Radio Architecture	SOSA™	OMS	JCA
Open Systems Focus	Portable Avionics SW Applications	Reusable HW Modules	Reusable HW Modules	Reusable HW/SW Modules	Mission Payload Reuse / Interchangeability	Portable and Reusable Avionics SW Applications
Sponsor	USN NAVAIR, USA PEO-Aviation, USAF AFLCMC	USN NAVAIR	N/A	USN NAVAIR, USA PEO Aviation, USAF AFLCMC	USAF AFLCMC	USA AMRDEC
Platform Domain	Avionics	Avionics	Avionics	Avionics (Payload)	Avionics (Mission System)	Avionics
Product Domain	SW	Embedded Computing	Communication Radios	Sensor Subsystems	Mission Payloads	SW Capabilities
Widely Adopted	Emerging	Emerging	No, Conceptual	In Development	Emerging	Emerging
Growth Path	Yes	Planned	TBD	Planned	Yes	TBD

Open IMA?

MOSA Open Standards vs Definitions

(Shepherd, K. and Jeremy Wills, J., “Avionics Open Systems Architecture Standardization”, AHS 74th Forum, 2018)



Avionics System Functional Definition

Application SW Module Definition

Data Interface Definition

Computing Environment Definition

HW Module Definition

Physical Interface Definition

HOST

FACE™

OMS

Open Radio

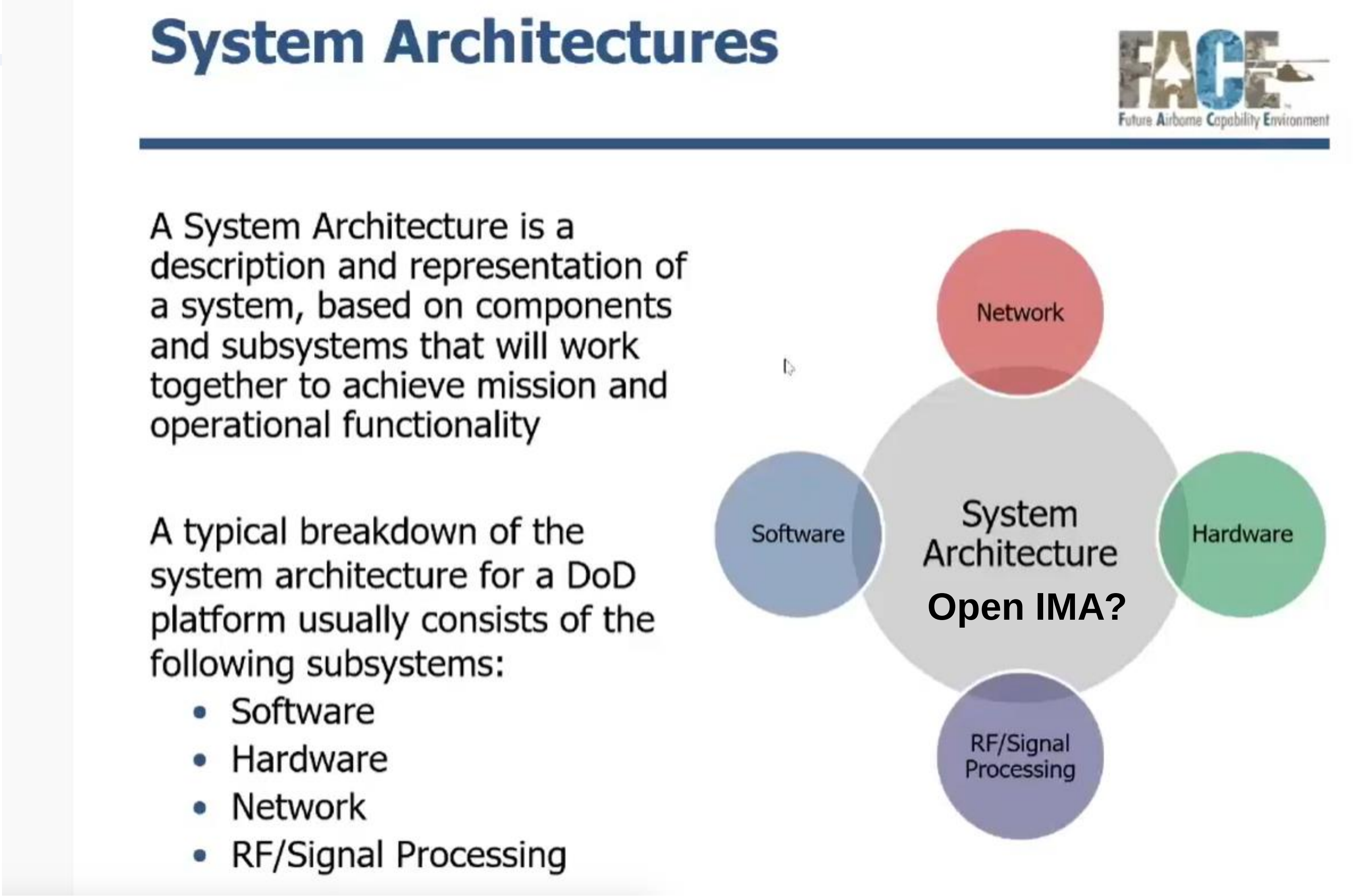
SOSA™

JCA

Certification
ARP 4754\
ARP 4761
DO178
DO-254
DO-297
OPEN IMA?

Open IMA should have been Included in the Joint Common Architecture (JCA) Report

- While DO 297 IMA was mentioned for Incremental Functional Certification (IFC) a more substantial assessment of Open IMA should have been includedl
- Recommend PEO Aviation MOSA Program conduct a revision of the JCA Report and include additional material on Open IMA
- Believe this would be a great addition for Open IMA bridging with MOSA
- Also believe the Civil-Military FSM DA Standard should be the Systems Integration Standard for the Open IMA System Integrator and the Platform Integrator



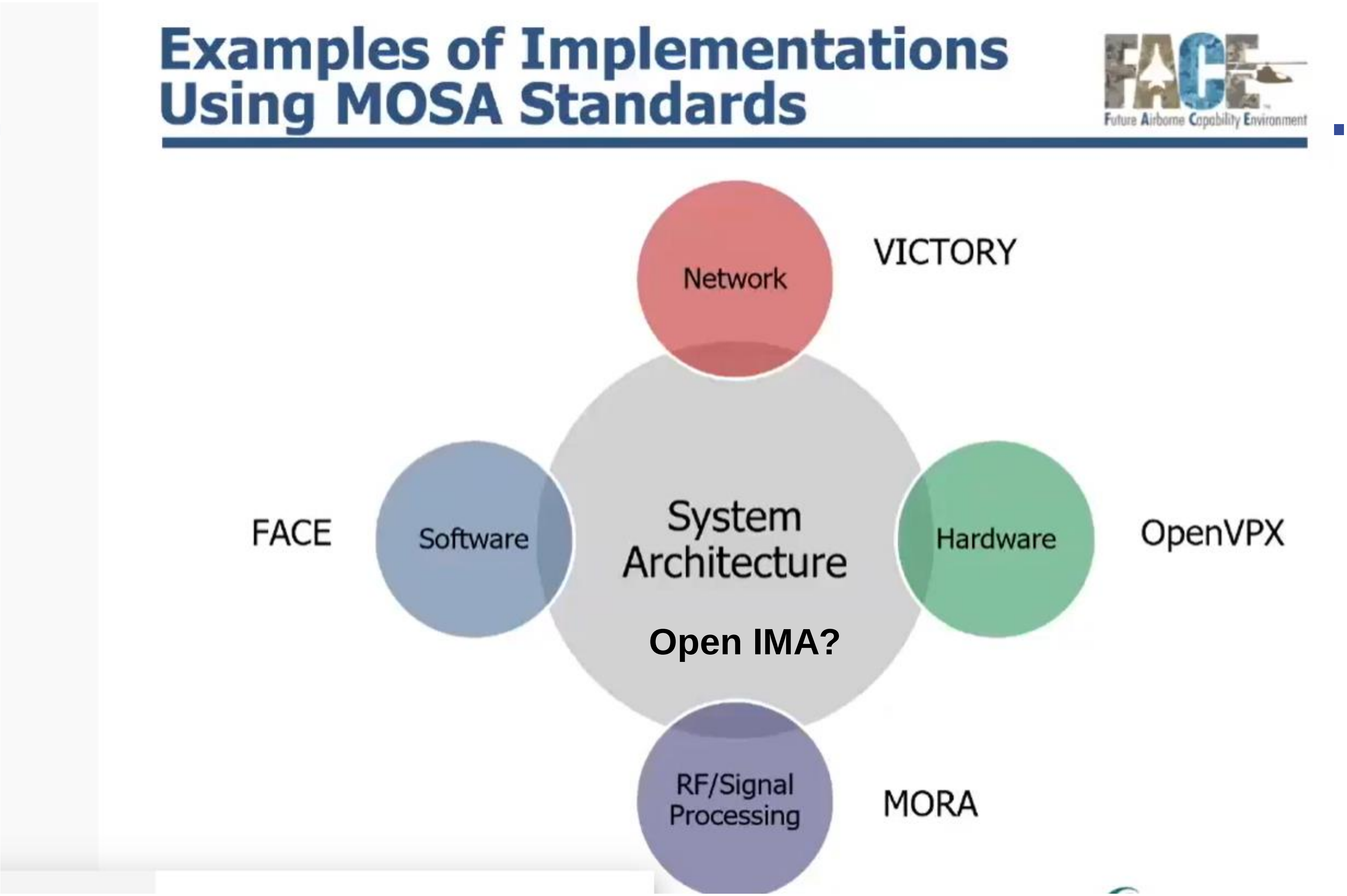
System Architectures

Future Airborne Capability Environment

A System Architecture is a description and representation of a system, based on components and subsystems that will work together to achieve mission and operational functionality

A typical breakdown of the system architecture for a DoD platform usually consists of the following subsystems:

- Software
- Hardware
- Network
- RF/Signal Processing



Examples of Implementations Using MOSA Standards

FACE Future Airborne Capability Environment

Network

VICTORY

FACE

Software

System Architecture

Hardware

OpenVPX

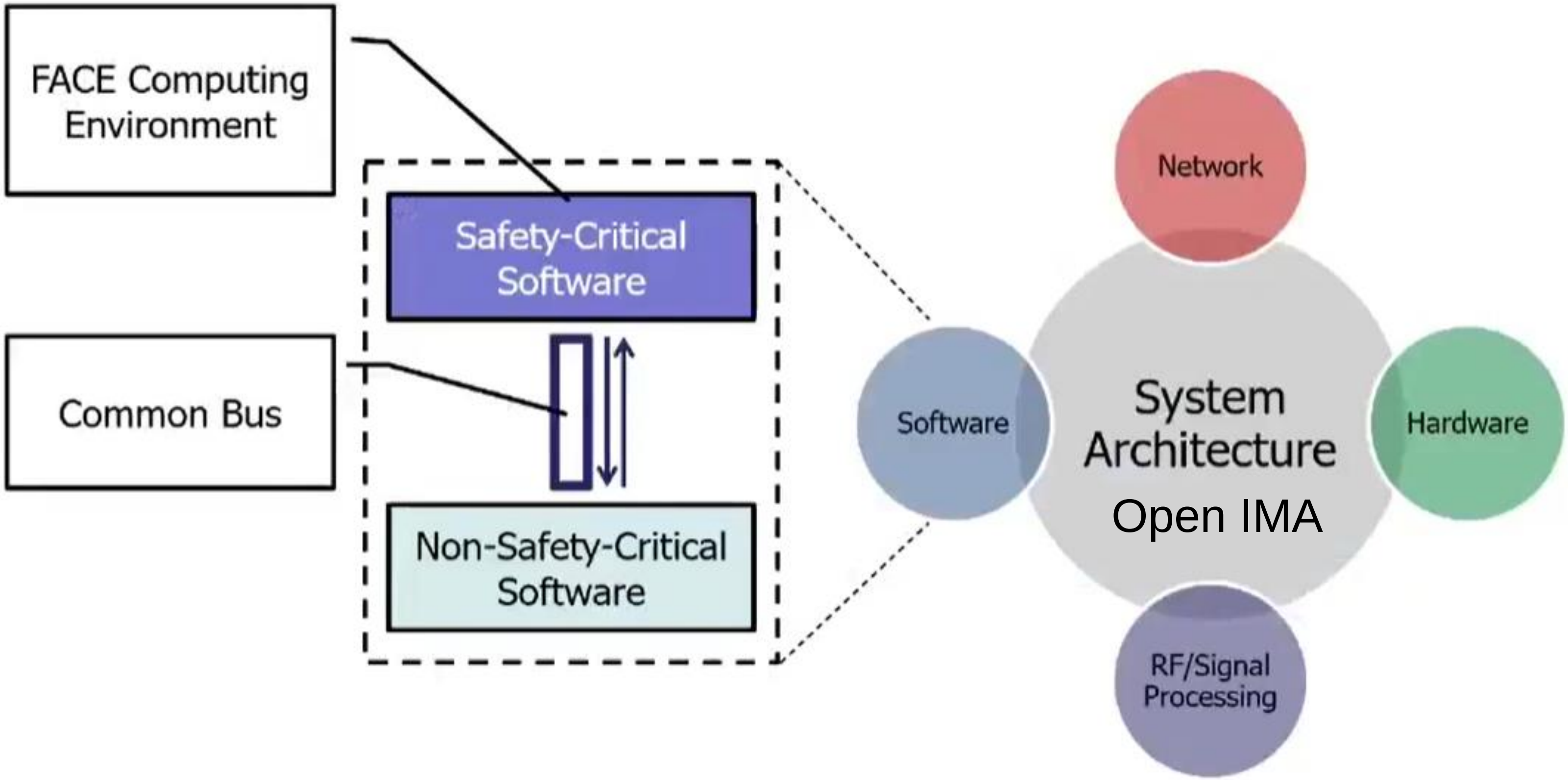
RF/Signal Processing

MORA

Open IMA?

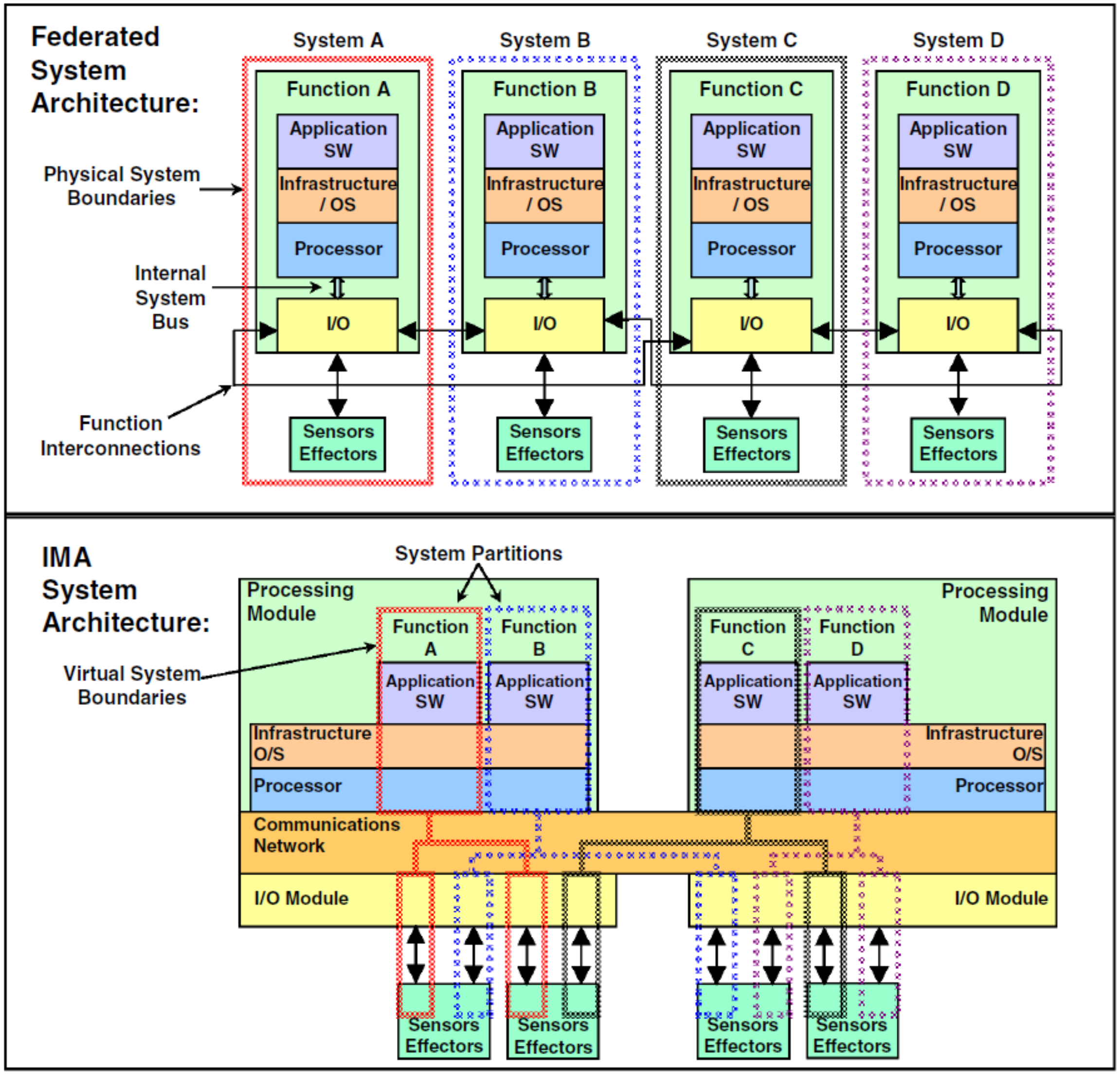
How the FACE Approach Fits into the Architecture Picture

FACE Approach by Itself Doesn't Address Open IMA and Run Time Assurance

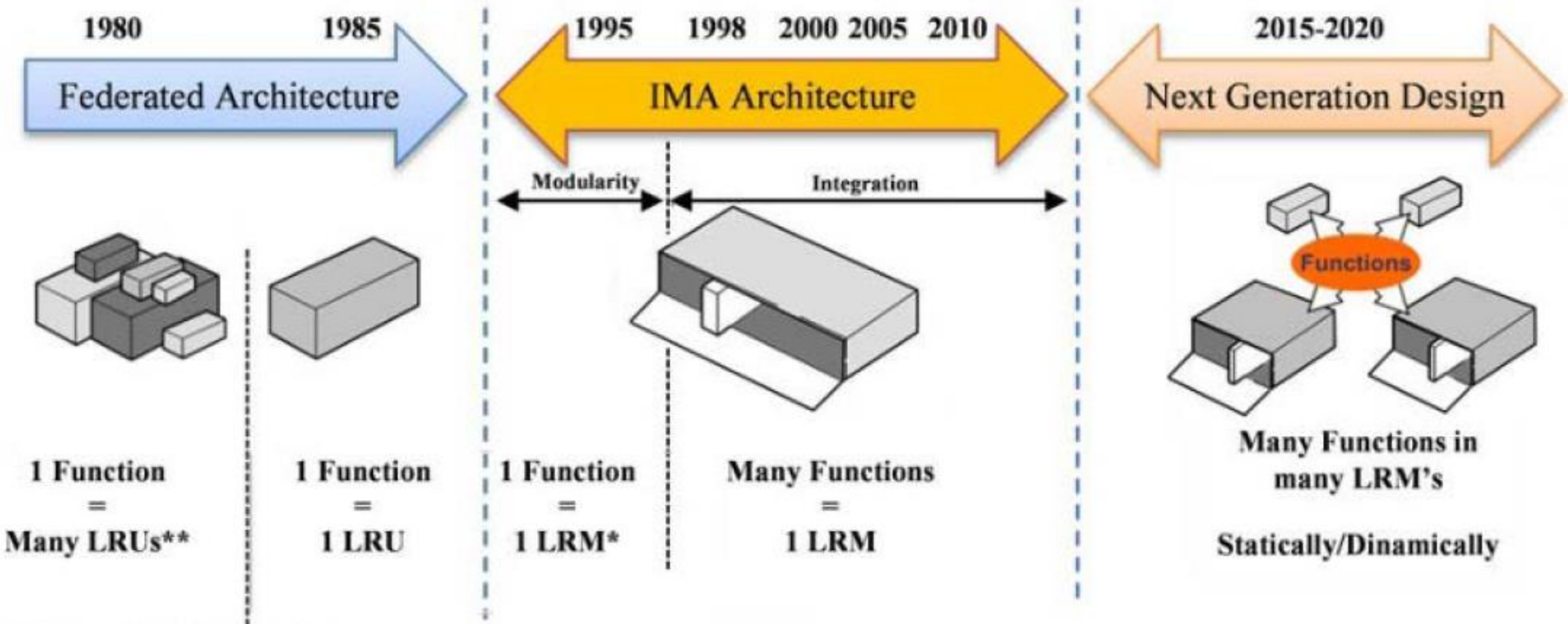


The FACE Technical Standard is a Component-Based Software Standard

Federated Versus Distributed Integrated Modular Avionics System Architectures

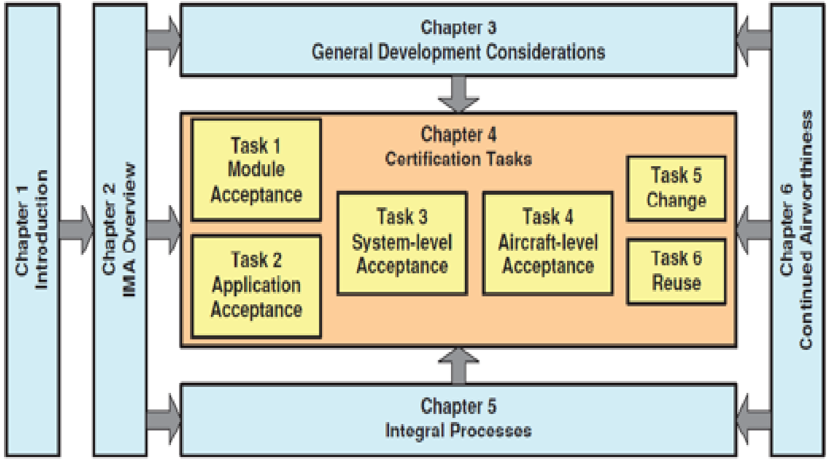


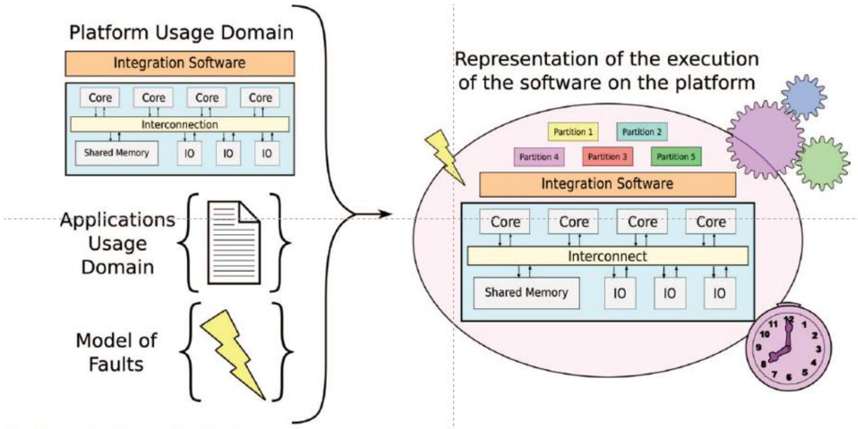
Rapid Evolution Taking Place From Federated Architecture to Open IMA Architecture for Multi-core Processor Designs



*Line replaceable module
**Line replaceable Unit

DO 297 IMA Tasks, Stakeholders and Implementation on ARINC 653 with Multi-Core Processors and Mandatory Requirements

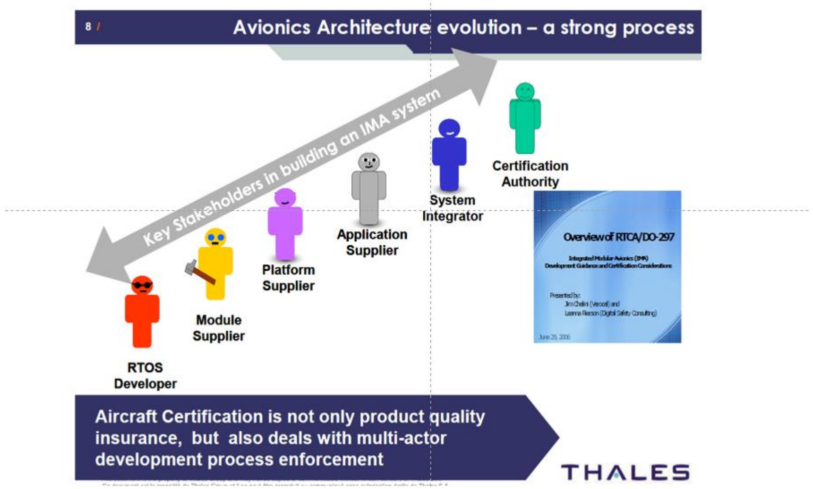




- Robust partitioning
- Platform determinism
- Platform limitations for WCET scenario definition

IMA Certification Requires Collaboration Between A Number of Stakeholders

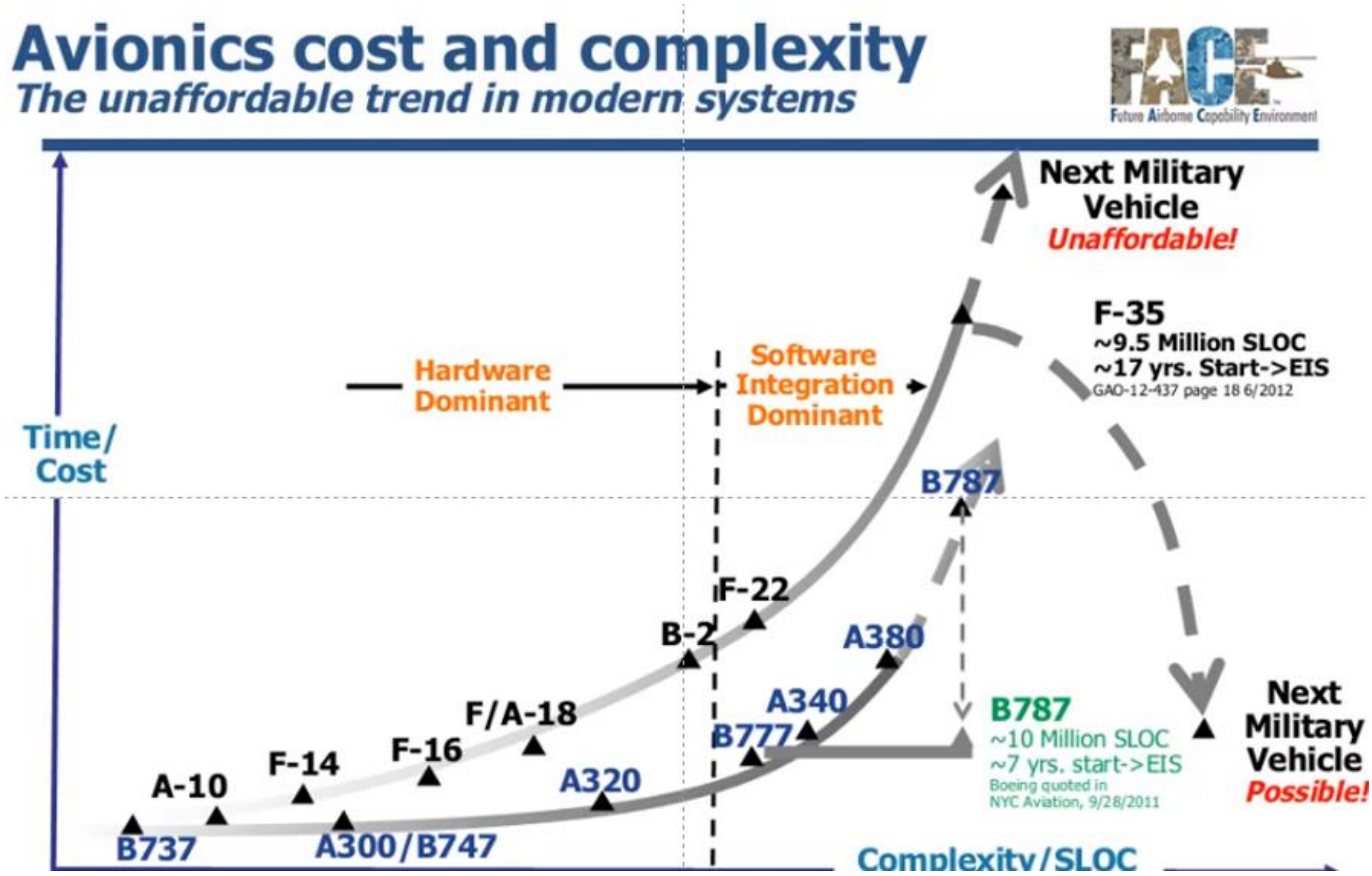
(Gatti, M. International Conference on Integrated Modular Avionics – MoscowThe EC FP7 R&D project: *SCARLETT*, 2012-10-29)



Aircraft Certification is not only product quality insurance, but also deals with multi-actor development process enforcement

- **Hardware/Software Integration**—The process of combining software into the target computer.
- **IMA System Integrator**—The developer who performs the activities necessary to integrate the platform(s), modules, and components with the hosted applications to produce the IMA system.
- **RTOS Supplier**—The RTOS supplier, as a member of the platform and module supplier role, has critical responsibilities of protectionwith regards to space, time, I/O, and other shared resources on the IMA system

A380 and B787 Aircraft have Reduced Avionics Cost & Complexity; F35 still trying to Transition



Avionics cost and complexity

The unaffordable trend in modern systems

B787 and A380 IMA Approaches

- While adapting the general concept of "shared resources," the Boeing 787 and the Airbus A380 approaches to IMA differ. Both aircraft have applications for specific LRUs that are on the plane and individual computers for certain systems
- Key to the B787 avionics suite, which Boeing developed with partners Smiths Aerospace, Rockwell Collins and Honeywell, is a central computing system Boeing calls the Common Core System (CCS), which eliminated more than 100 different LRUs.
- The A380 Super Jumbo is called an Open IMA, which touts 15 to 20 percent lower operating costs than previous airliners, applies the IMA concept with computers capable of hosting different functions and integrated modular avionics connected by a network. This approach differs from Boeing’s 787 central computing system in that it does not rely on a single (or dual) central processor to run most of the aircraft systems.

What is an Open IMA? How Each Role Can Help The Others – GE Aviation Systems, IEEE A&E SYSTEMS MAGAZINE, JANUARY 2010

- **The development, certification, and maintenance of an Integrated Modular Avionics (IMA) system is divided into distinct roles (as defined in DO-297) as follows**:

  1. Development • IMA System Integrator • Platform and Module Suppliers • Application Supplier

  2. Certification • Certification Authority • Certification Applicant

  3. Maintenance Organization

- **This focuses on the development portion of an Open IMA system life-cycle**, which is typically performed by several different companies. The number involved in developing an IMA system can reach into the thousands, making effective communication and prioritization of work between development roles and companies essential for meeting project deadlines and goals

- **This provides a set of recommendations from each of the IMA development roles,** for how their development activities could be optimized by the actions (or development process) of those performing the other IMA development roles. **These suggestions were drawn from GE Aviation's experience as an IMA System Integrator, Platform Supplier, and Application Supplier on numerous Open IMA development programs**

What is an Open IMA? How Each Role Can Help The Others – GE Aviation Systems, Based on a presentation at DASC2008

- **IMA System Integrator Recommendations**
  The IMA system integrator performs the activities necessary to integrate the platform(s) and hosted applications to produce the IMA system. Typical data developed during IMA system integration includes :
  - The system configuration consisting of the number, type, and specific versions of modules and hosted applications.
  - The shared resource allocation and configuration tables for the integrated IMA system.
  - Results of IMA system V&V, including performance data for the IMA system, consistent with the allocated requirements.

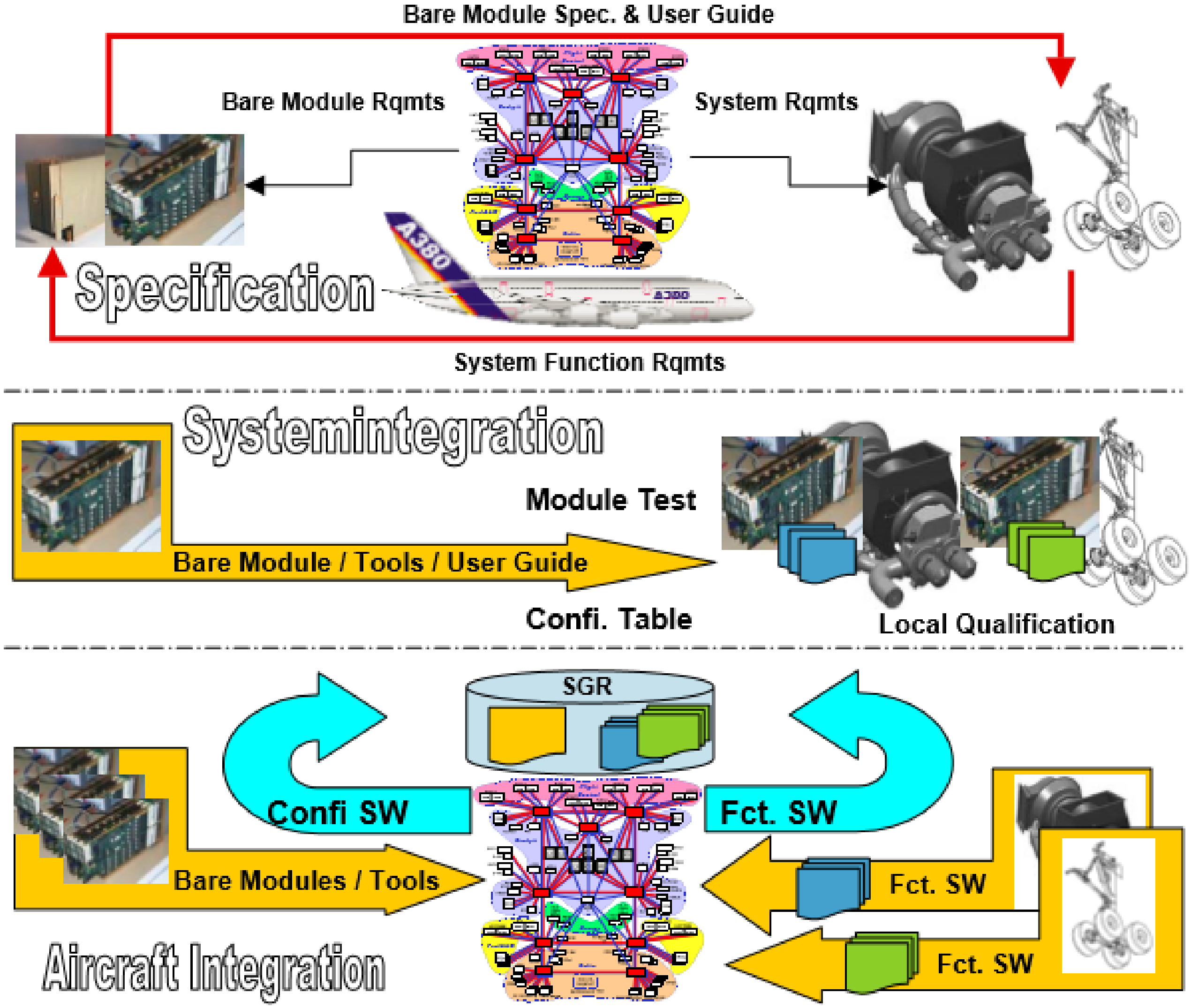
What is an Open IMA? How Each Role Can Help The Others – GE Aviation Systems, Based on a presentation at DASC2008

The following list highlights the recommendations that the System Integrator would like to see implemented by the **Platform Supplier** and **Application Supplier** in order to optimize the IMA System development and integration.

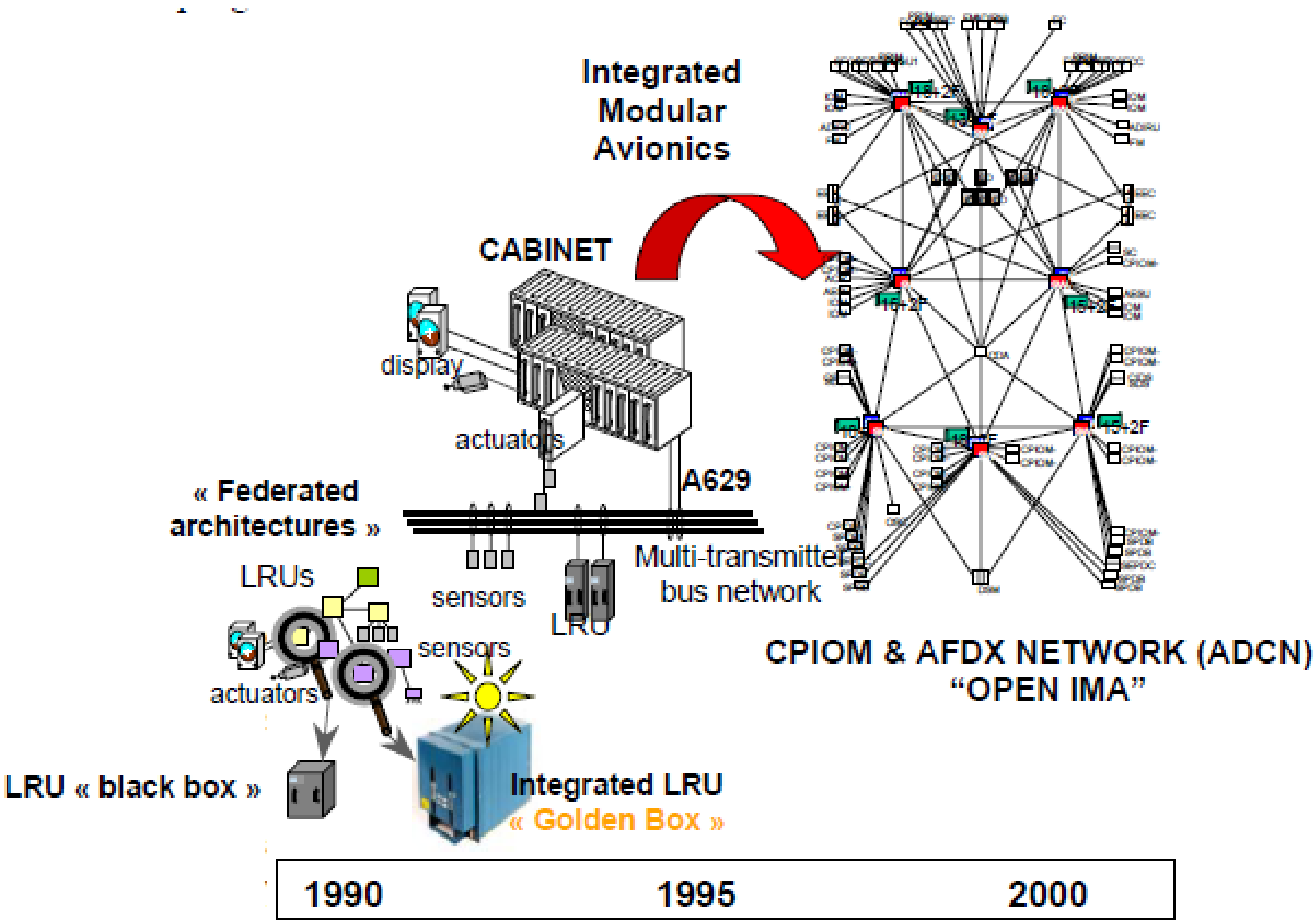
1. **The Platform Supplier should provide a data package** (early in the development phase of the program) that accurately documents the attributes of the Platform. This data package will enable the **System integrator** to develop a system architecture, develop Application Supplier procurement packages, and work with **Application Suppliers** to develop a system architecture that optimizes the system at the aircraft level.

Areas of focus for this data package are: **Software APIs**; **Software Development Environment (SDE); I/O interfaces; Test Environment; Performance characteristics and tools to help estimate resource usage; Physical characteristics, and Safety characteristics**.

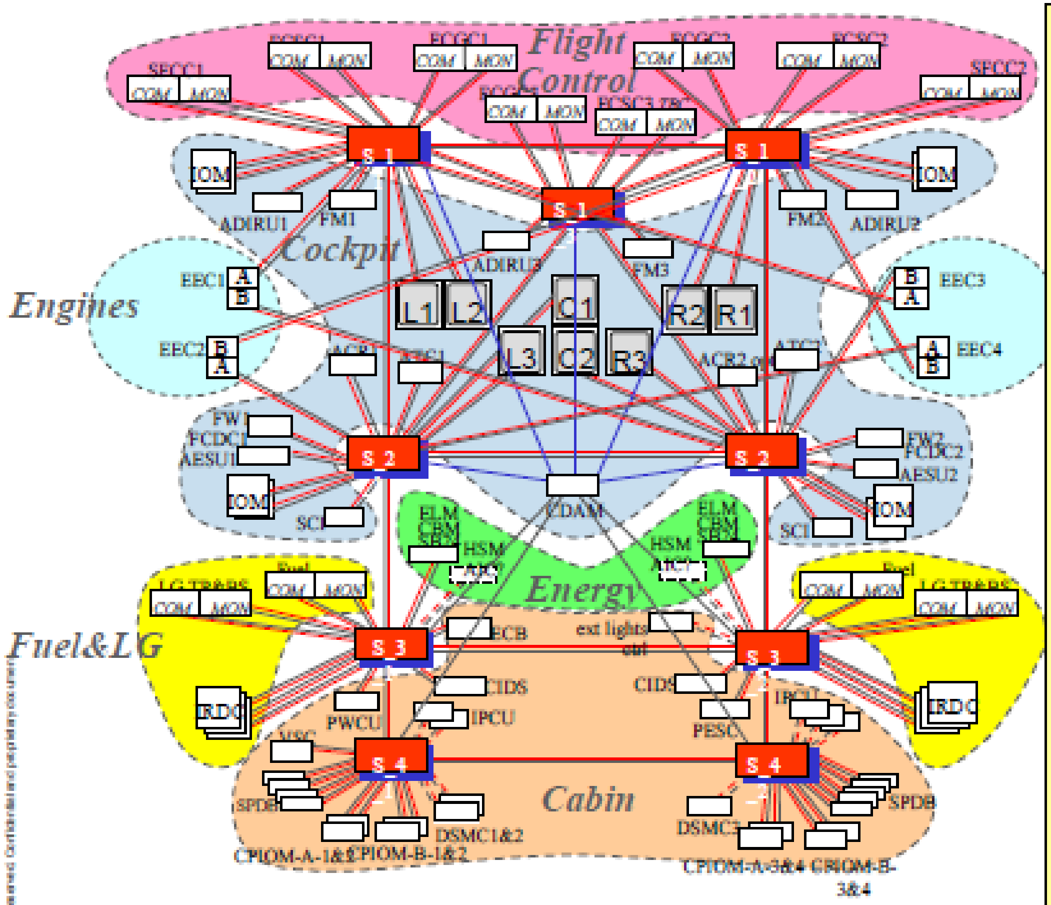
Development and Functions to Open IMA First Generation (IMA1G) Network Integration Processes Required a New Integration Approach, Airbus 380 (Butz, H., AirBus)



Open Integrated Modular Avionic (IMA): State of the Art and Future Development Road (Butz, H. Airbus 2013)



What is A380 IMA? ADCN Network &Topology (Butz, H. Airbus 2013)



AFDX Network:

- 100 Mbits
- Redundant Network (A&B) with independent alimentation
- AFDX switches = 2 x 8
- NB of ports (connections) possible on each switch (20-24)
- MTBF of the switch is very high (100 000 hours expected)
- Up 80 AFDX subscriber

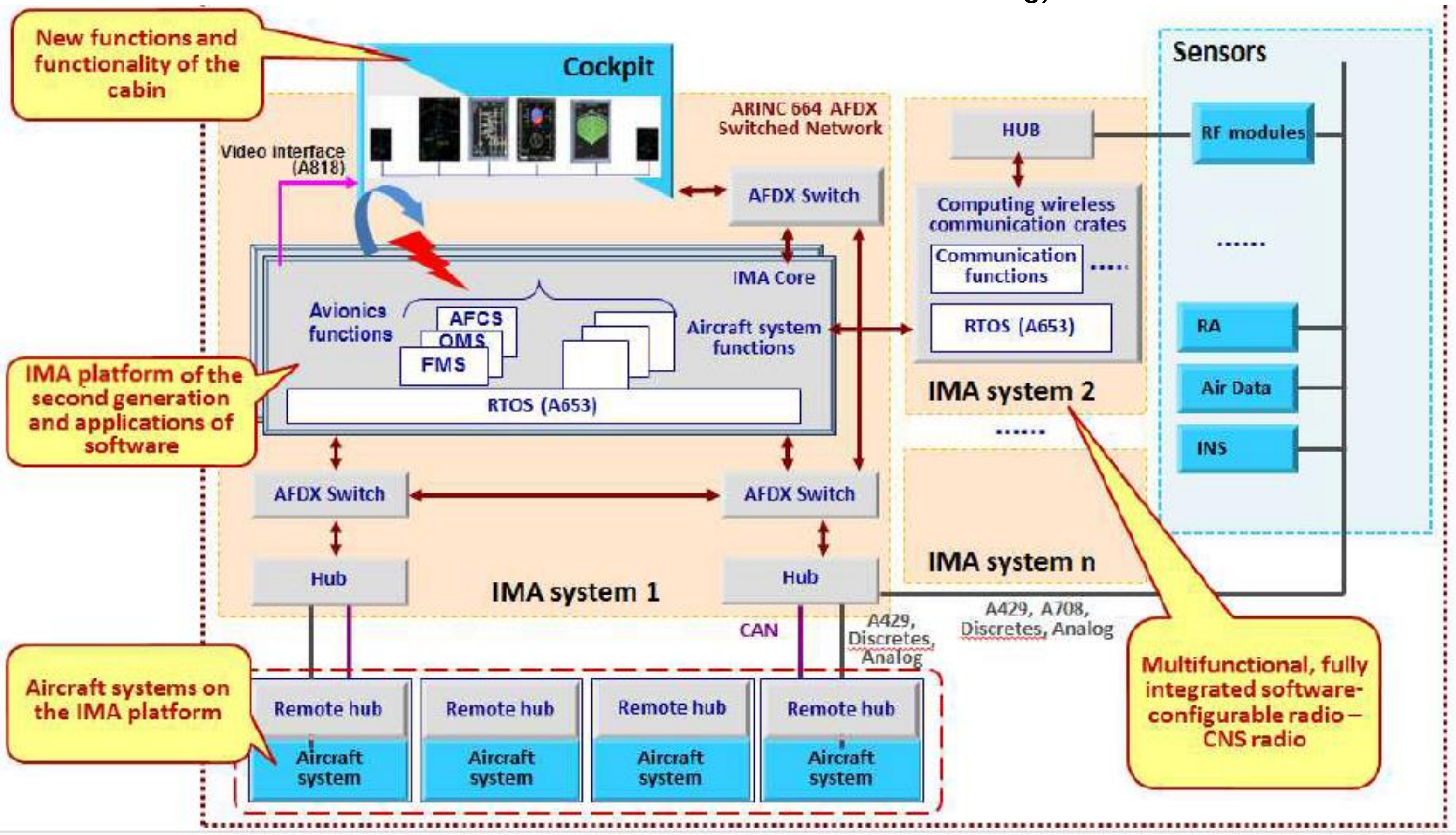
European Union IMA Avionics Research Programs over the past decade (2010-2020)

- Two joint research programs in IMA were funded in Europe over the Past Decade
  - The Scarlett Program started in the early 2000s and developed the first generation IMA called IMA1G
  - The Ashley Program was a follow-on to develop a second generation Open IMA designated as IMA2G
- Illustrated in the next chart is an illustration of an Open IMA2G with separate IMAs for different Subsystem Functions

European Community Pursued IMA2G through SCARLETT & ASHLEY Programs (2010-2020)

Example Modern 2nd Gen IMA Network architecture

(Chuyanov, G.A., et al, Advanced Avionics Equipment on the Basis of 2nd Generation Integrated Modular Avionics, ICAS 2014, St. Petersburg)



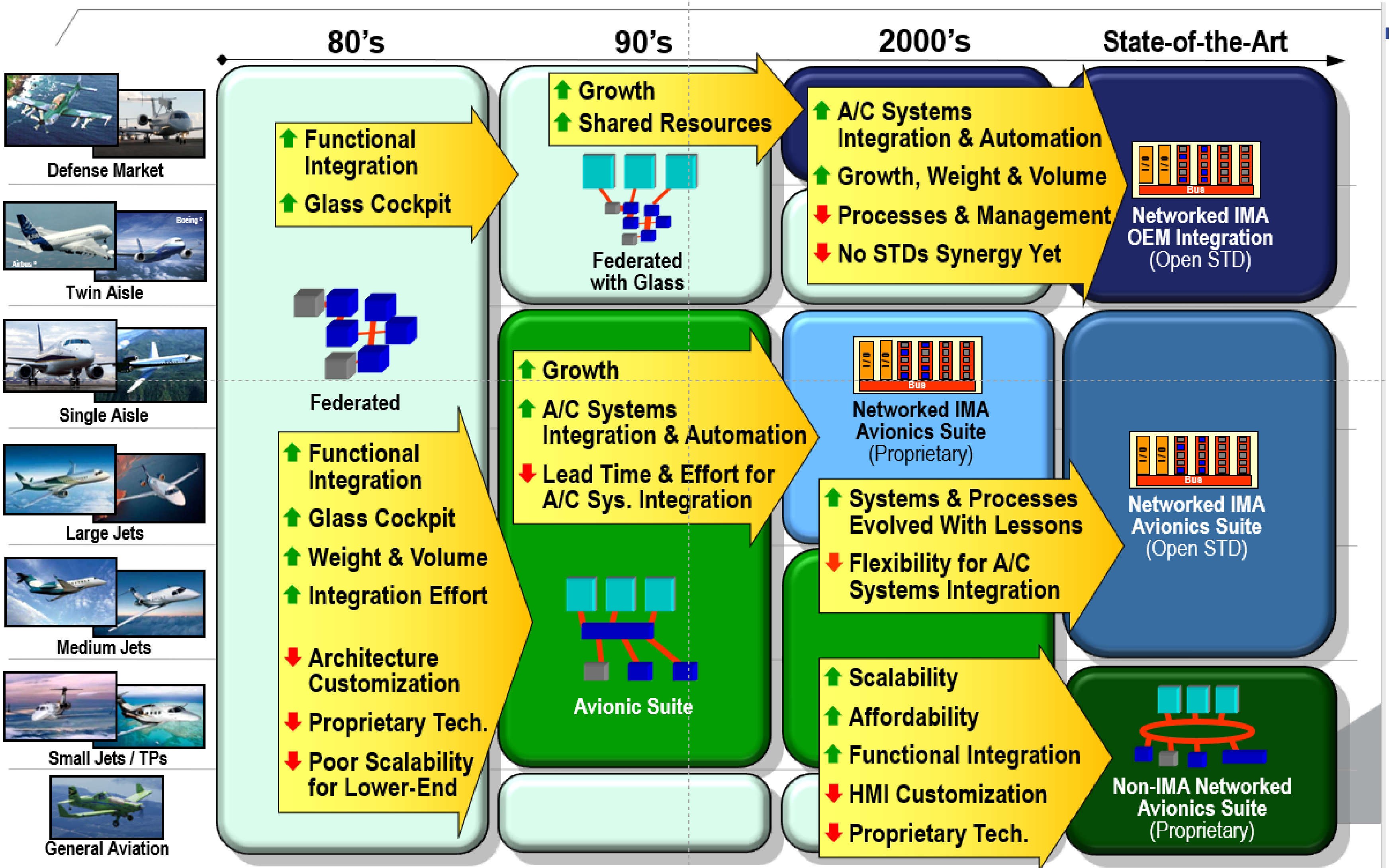
Embraer Transition to Open IMA is ongoing example

Aircraft Systems Integration from EMBRAER Perspective

João Paulo Marques Reginato – Systems Integration Manager

31/August/2015

Embraer Notional Evolution to State-of-the Art



80's | 90's | 2000's | State-of-the-Art

Defense Market

Twin Aisle

Single Aisle

Large Jets

Medium Jets

Small Jets / TPs

General Aviation

↑ Functional Integration
↑ Glass Cockpit

Federated

↑ Functional Integration
↑ Glass Cockpit
↑ Weight & Volume
↑ Integration Effort
↓ Architecture Customization
↓ Proprietary Tech.
↓ Poor Scalability for Lower-End

↑ Growth
↑ Shared Resources

Federated with Glass

↑ Growth
↑ A/C Systems Integration & Automation
↓ Lead Time & Effort for A/C Sys. Integration

Avionic Suite

↑ A/C Systems Integration & Automation
↑ Growth, Weight & Volume
↓ Processes & Management
↓ No STDs Synergy Yet

Networked IMA OEM Integration (Open STD)

Networked IMA Avionics Suite (Proprietary)

↑ Systems & Processes Evolved With Lessons
↓ Flexibility for A/C Systems Integration

Networked IMA Avionics Suite (Open STD)

↑ Scalability
↑ Affordability
↑ Functional Integration
↓ HMI Customization
↓ Proprietary Tech.

Non-IMA Networked Avionics Suite (Proprietary)

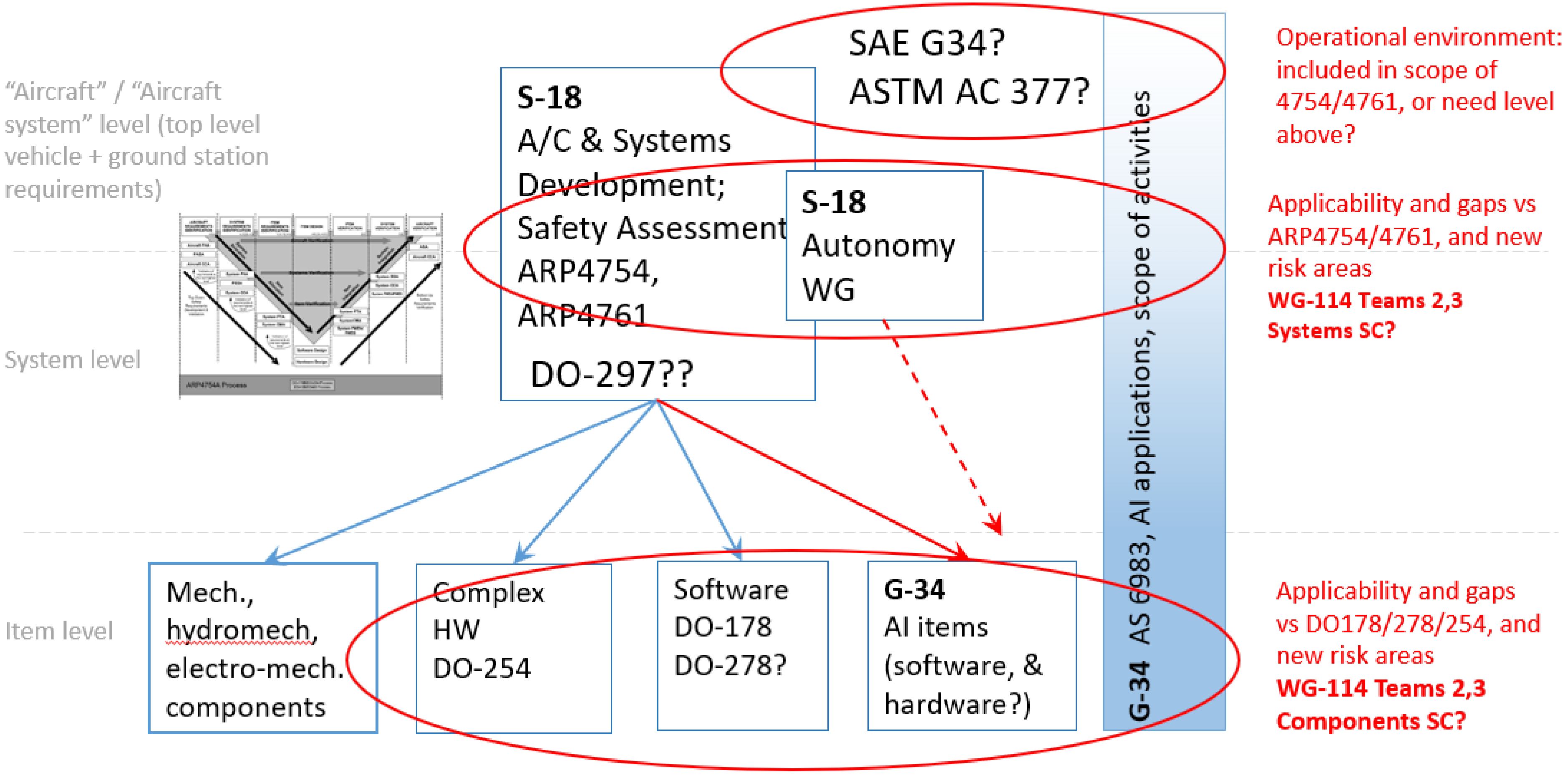
This chart is notional and does not refer to any industry milestones such as aircraft launch, certification or entry into service dates. It's only intended to provide a big picture of the avionics evolution.

Lockheed Again Lowers F-35 Delivery Guidance On New Upgrade: F-35 PMO and GE Aviation Systems Now Involved

Steve Trimble September 06, 2023

- **Lockheed Martin has further delayed delivery of the first F-35 upgraded with new avionics, to the second quarter of 2024, adding more jets to a backlog of deferred shipments since 2020, the company announced on Sept. 6.**
- The latest schedule slip means Lockheed now expects to deliver only 97 F-35s this year, a further reduction from an estimate in July of 100-200.
- The company originally planned to deliver 147-153.
- **The delays are being caused by scheduling with an ongoing certification process for the software in the Technology Refresh-3 (TR-3) hardware**, which includes an L3Harris integrated core processor, an aircraft memory unit and an RTX electro-optical distributed aperture system, Lockheed says in a new regulatory filing.
- L3Harris and RTX have also fallen behind on deliveries of TR-3 hardware.

SAE Standards are Continuously being Updated



"Aircraft" / "Aircraft system" level (top level vehicle + ground station requirements)

System level

Item level

SAE G34?
ASTM AC 377?

S-18
A/C & Systems Development; Safety Assessment
ARP4754,
ARP4761

DO-297??

S-18
Autonomy WG

Mech., hydromech, electro-mech. components

Complex HW
DO-254

Software
DO-178
DO-278?

G-34
AI items (software, & hardware?)

G-34 AS 6983, AI applications, scope of activities

Operational environment: included in scope of 4754/4761, or need level above?

Applicability and gaps vs ARP4754/4761, and new risk areas
WG-114 Teams 2,3 Systems SC?

Applicability and gaps vs DO178/278/254, and new risk areas
WG-114 Teams 2,3 Components SC?

Civil Transport Aircraft FSM DA Standards, 2010

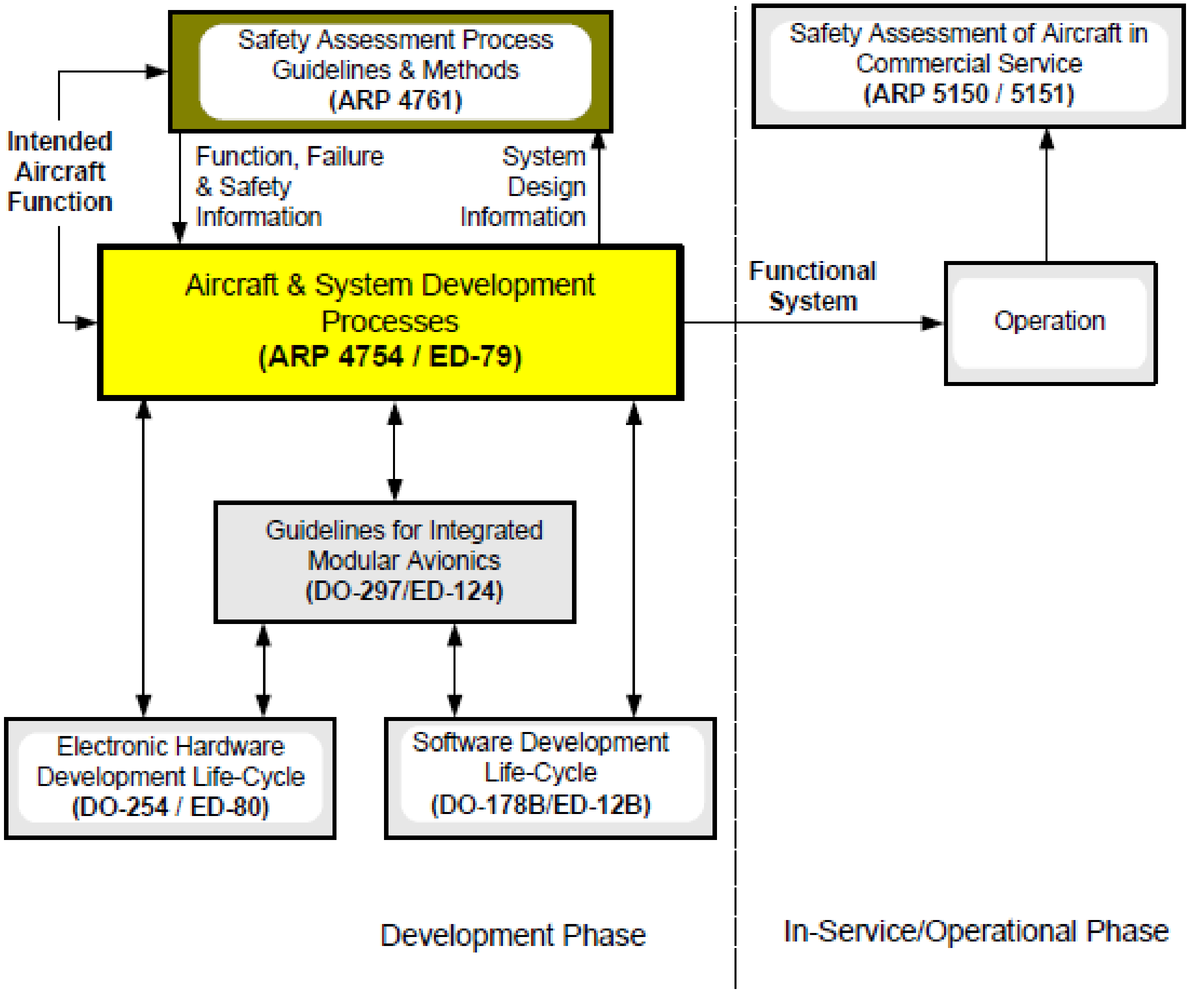
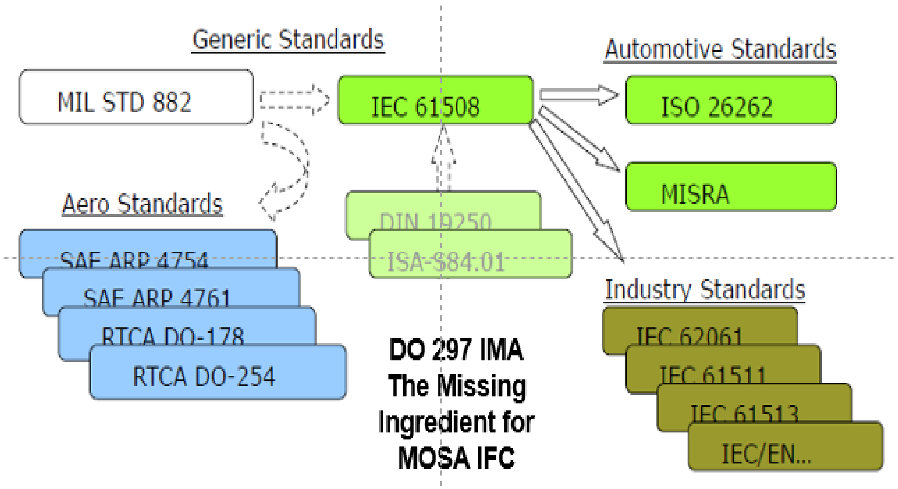
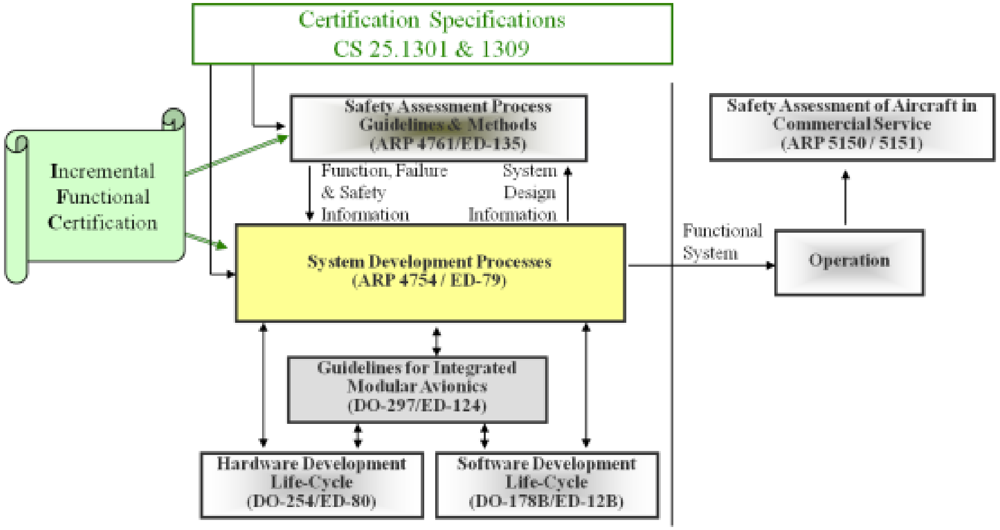

Safety Assessment Process Guidelines & Methods (ARP 4761)
Intended Aircraft Function
Function, Failure & Safety Information
System Design Information
Aircraft & System Development Processes (ARP 4754 / ED-79)
Guidelines for Integrated Modular Avionics (DO-297/ED-124)
Electronic Hardware Development Life-Cycle (DO-254 / ED-80)
Software Development Life-Cycle (DO-178B/ED-12B)
Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)
Functional System
Operation
Development Phase
In-Service/Operational Phase

FIGURE 1 - GUIDELINE DOCUMENTS COVERING DEVELOPMENT AND IN-SERVICE/OPERATIONAL PHASES

Incremental Functional Certification (IFC) with Multi-Core Processors(MPCs) is a Key for SWAP Reduction and Assured Autonomy




Certification Specifications
CS 25.1301 & 1309
Incremental Functional Certification
Safety Assessment Process Guidelines & Methods (ARP 4761/ED-135)
Function, Failure & Safety Information
System Design Information
System Development Processes (ARP 4754 / ED-79)
Guidelines for Integrated Modular Avionics (DO-297/ED-124)
Hardware Development Life-Cycle (DO-254/ED-80)
Software Development Life-Cycle (DO-178B/ED-12B)
Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)
Functional System
Operation

Guidelines are Available for the Military to Apply Civil Aviation Development, Safety and Certification

Esterline

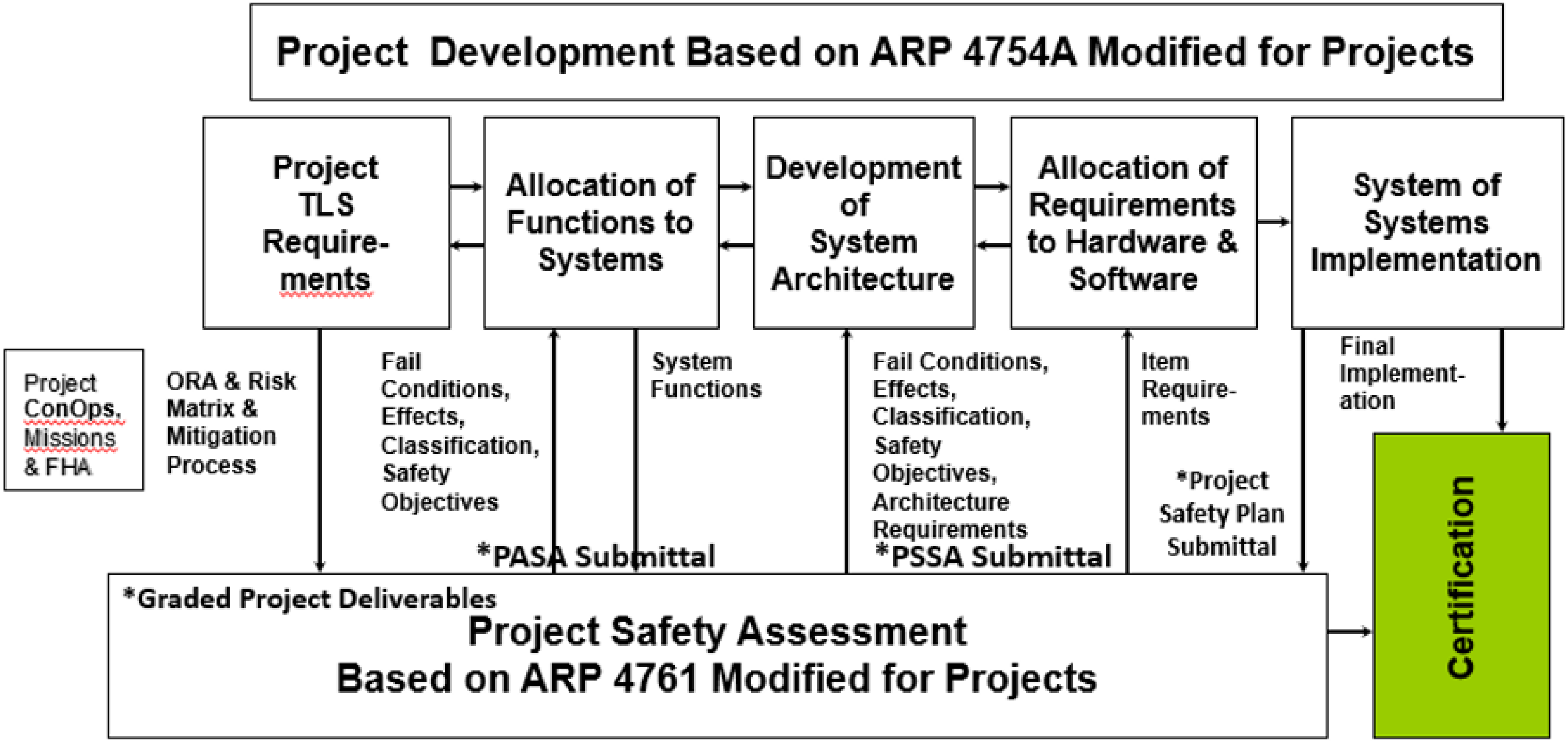
Control Systems

Guidelines for Development of Civil Aircraft and Systems

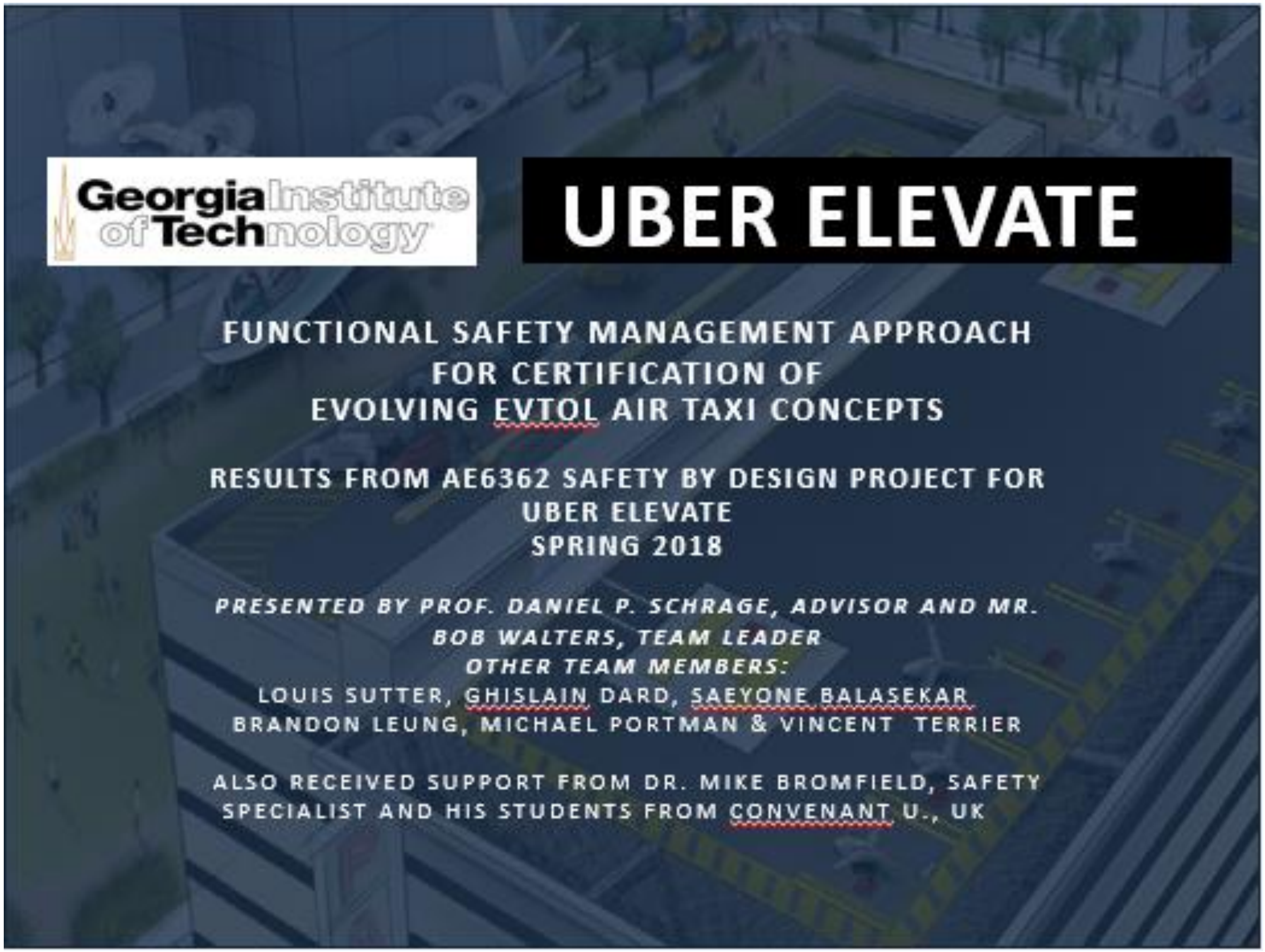
Introduction to ARP4754A

23 July, 2014

Taught & Modified Safety by Design & Flight Certification Course for 30 Years
AE636219 FSM Approach with Identified Project Deliverables
Modified for It for Military Aircraft, UAS, eVTOL and Autonomy


Project Development Based on ARP 4754A Modified for Projects
Project TLS Require-ments
Allocation of Functions to Systems
Development of System Architecture
Allocation of Requirements to Hardware & Software
System of Systems Implementation
Project ConOps, Missions & FHA
ORA & Risk Matrix & Mitigation Process
Fail Conditions, Effects, Classification, Safety Objectives
System Functions
Fail Conditions, Effects, Classification, Safety Objectives, Architecture Requirements
Item Require-ments
Final Implement-ation
*PASA Submittal
*PSSA Submittal
*Project Safety Plan Submittal
*Graded Project Deliverables
Project Safety Assessment
Based on ARP 4761 Modified for Projects
Certification

AE6362 2018 Safety By Design & Flight Certification Project for Uber Elevate Uber Elevate Air Taxi Project



Georgia Institute of Technology

UBER ELEVATE

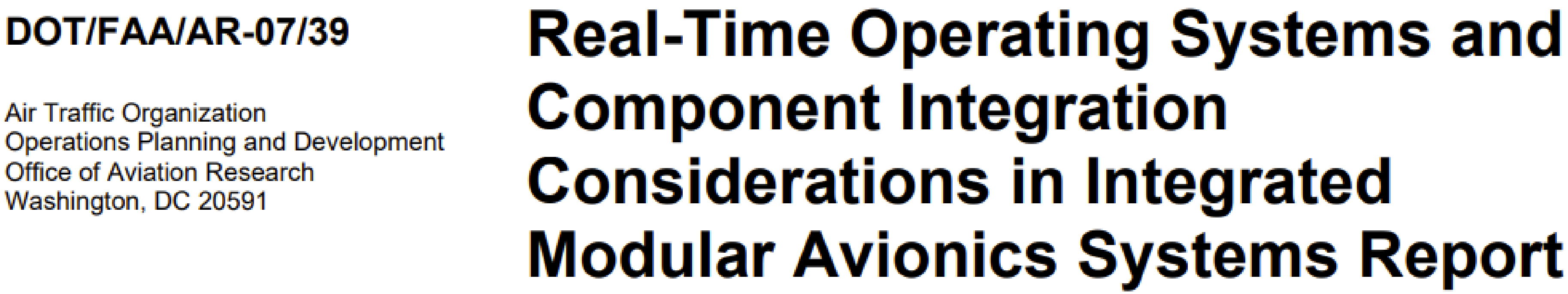
FUNCTIONAL SAFETY MANAGEMENT APPROACH
FOR CERTIFICATION OF
EVOLVING EVTOL AIR TAXI CONCEPTS

RESULTS FROM AE6362 SAFETY BY DESIGN PROJECT FOR
UBER ELEVATE
SPRING 2018

PRESENTED BY PROF. DANIEL P. SCHRAGE, ADVISOR AND MR.
BOB WALTERS, TEAM LEADER
OTHER TEAM MEMBERS:
LOUIS SUTTER, GHISLAIN DARD, SAEYONE BALASEKAR
BRANDON LEUNG, MICHAEL PORTMAN & VINCENT TERRIER

ALSO RECEIVED SUPPORT FROM DR. MIKE BROMFIELD, SAFETY SPECIALIST AND HIS STUDENTS FROM CONVENANT U., UK

Understanding How Open IMA can be Implemented

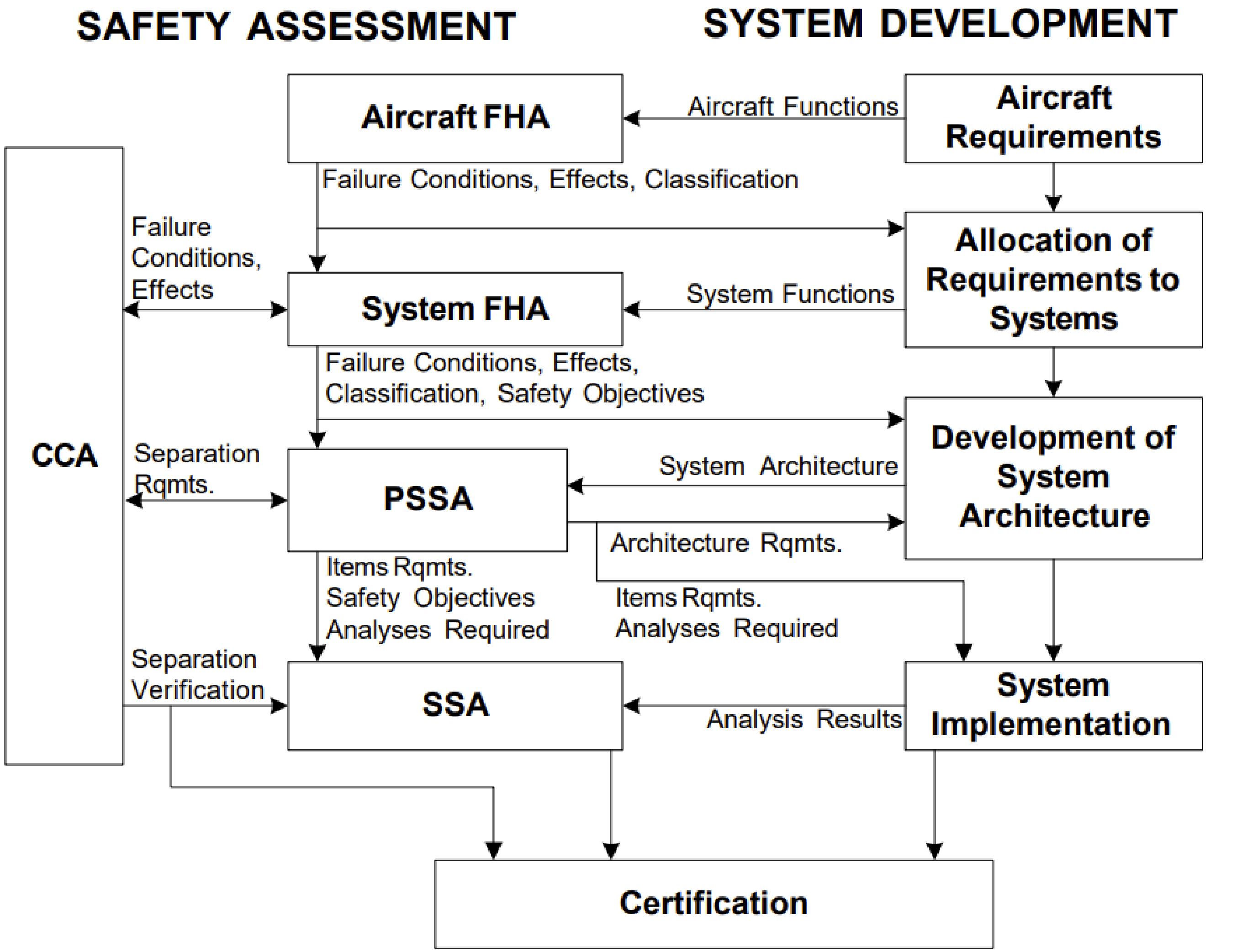


DOT/FAA/AR-07/39

Air Traffic Organization
Operations Planning and Development
Office of Aviation Research
Washington, DC 20591

Real-Time Operating Systems and Component Integration Considerations in Integrated Modular Avionics Systems Report

Figure 1. ARP 4754 Safety Assessment and System Development Processes



SAFETY ASSESSMENT

SYSTEM DEVELOPMENT

Aircraft FHA

Aircraft Functions

Aircraft Requirements

Failure Conditions, Effects, Classification

Failure Conditions, Effects

Allocation of Requirements to Systems

System FHA

System Functions

Failure Conditions, Effects, Classification, Safety Objectives

CCA

Separation Rqmts.

PSSA

System Architecture

Development of System Architecture

Architecture Rqmts.

Items Rqmts. Safety Objectives Analyses Required

Items Rqmts. Analyses Required

Separation Verification

SSA

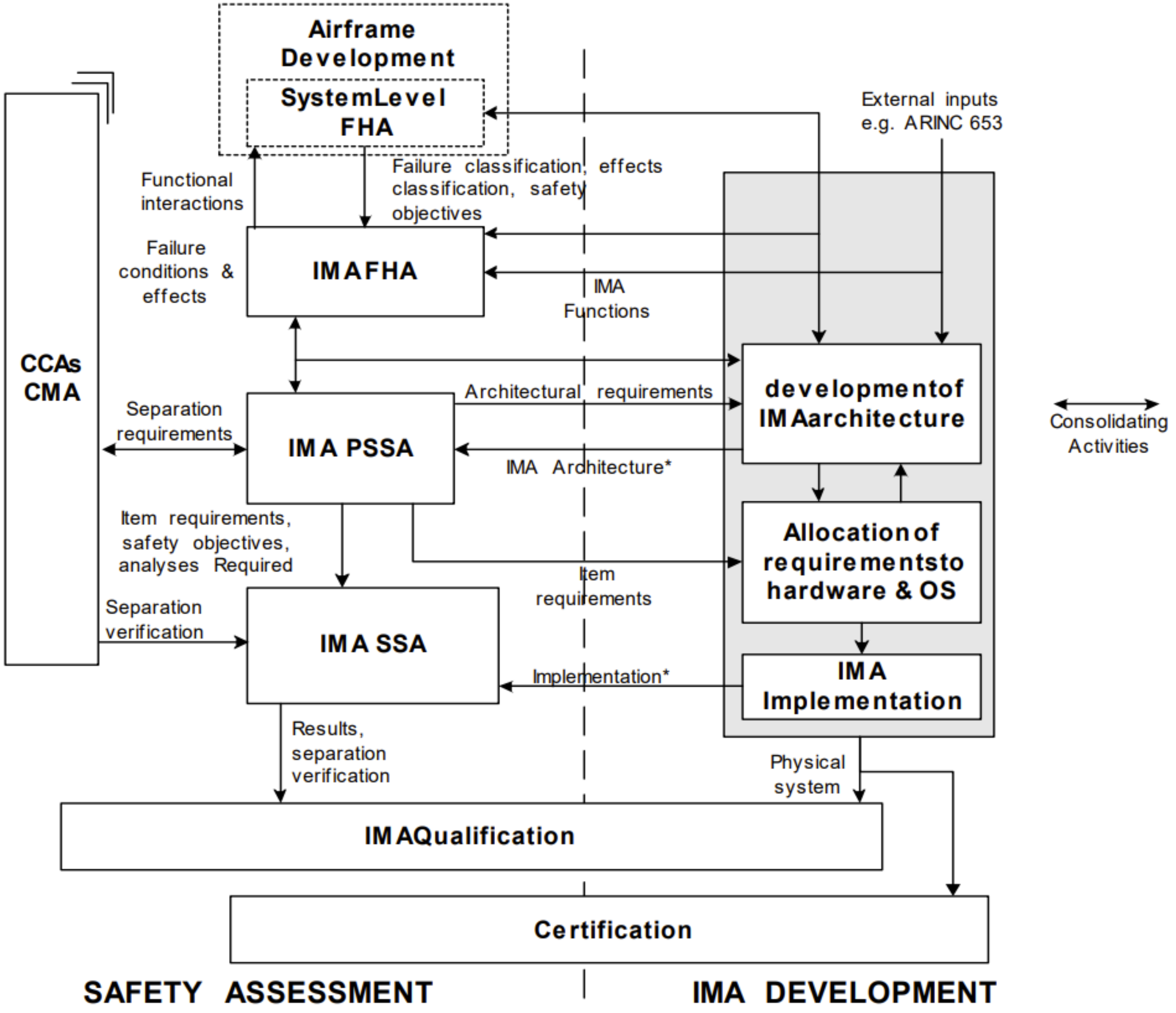
Analysis Results

System Implementation

Certification

(Taken from ARP 4754)

Figure 2. The IMA System Certification Considerations



ARINC 653 Basic Architecture

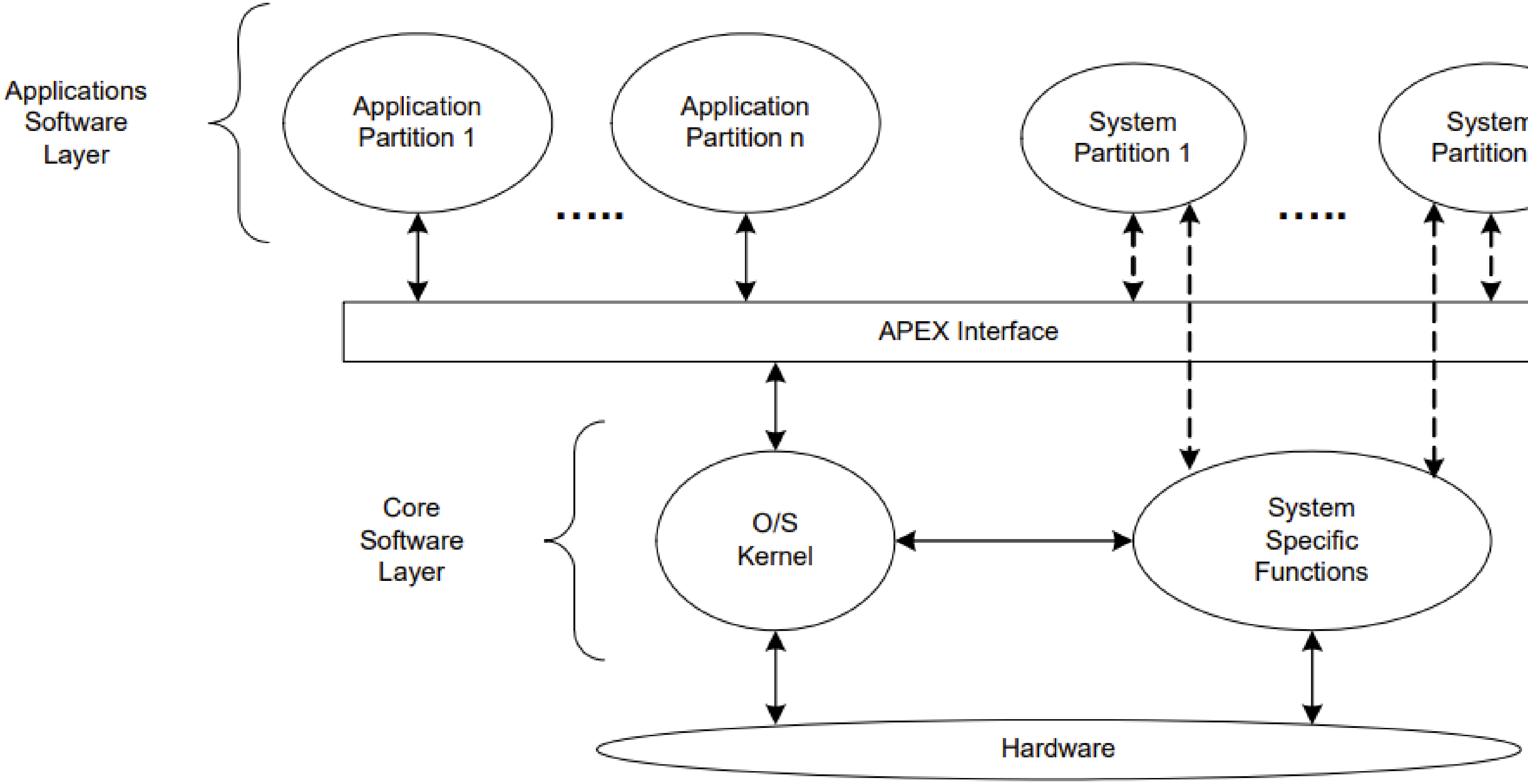
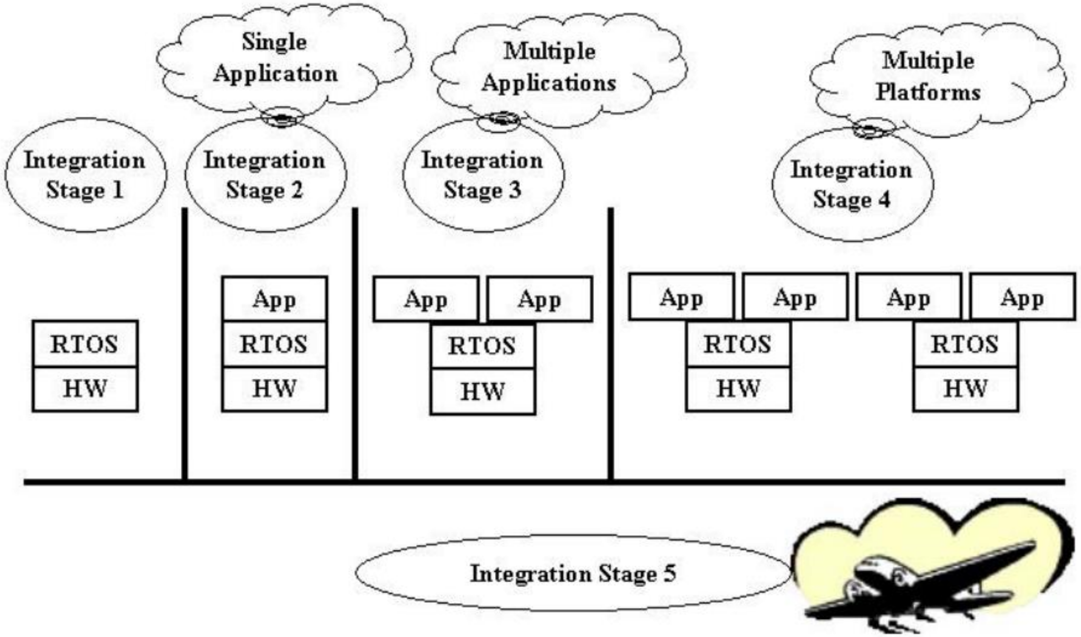
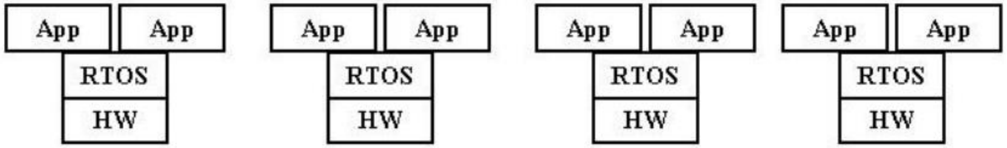


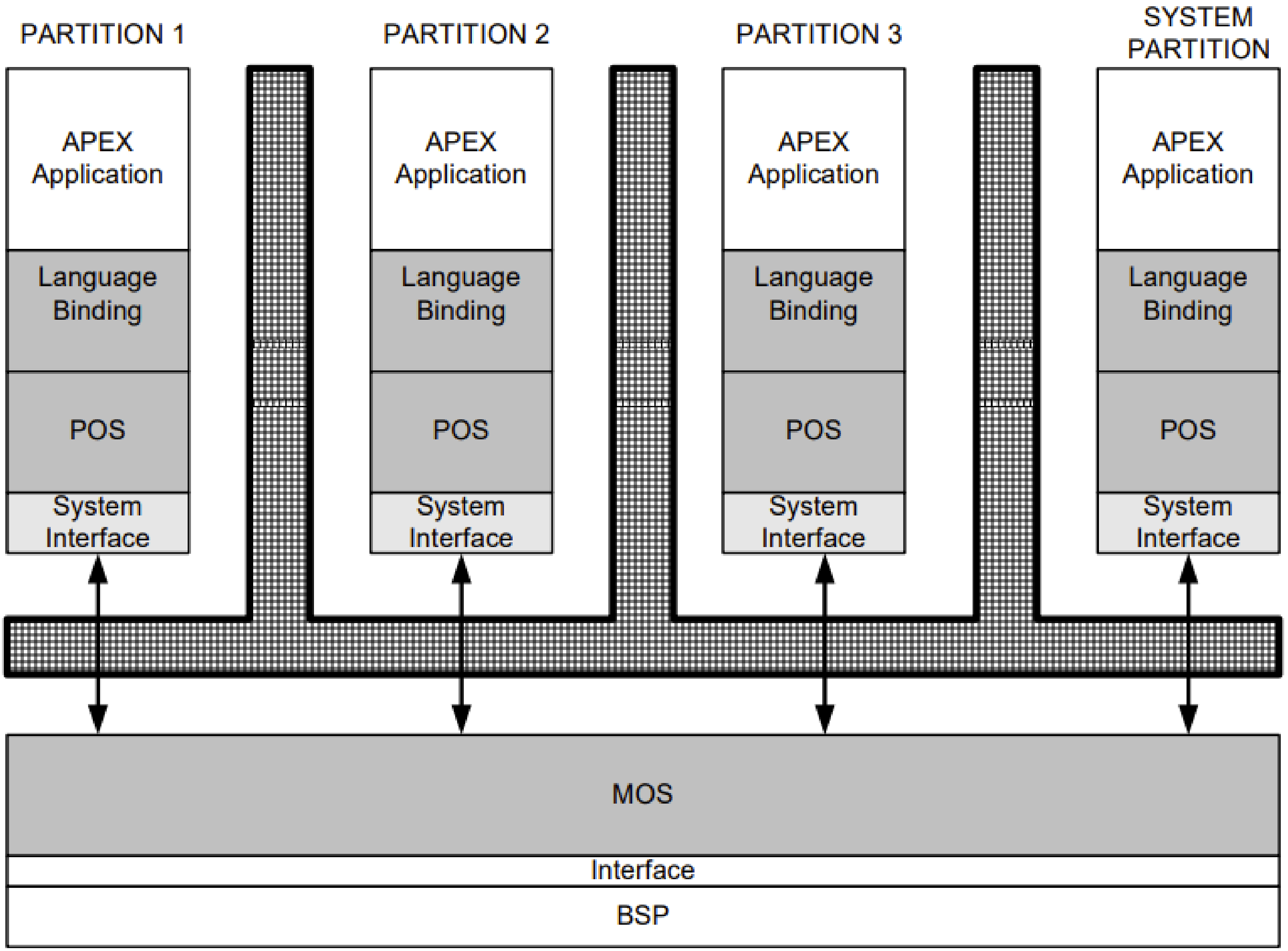
Figure 4. Staged Integration View of IMA System Development



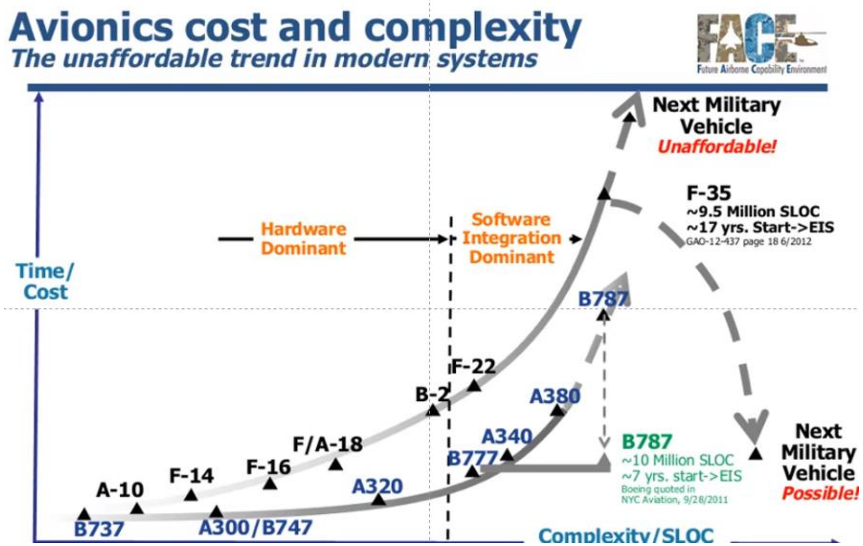


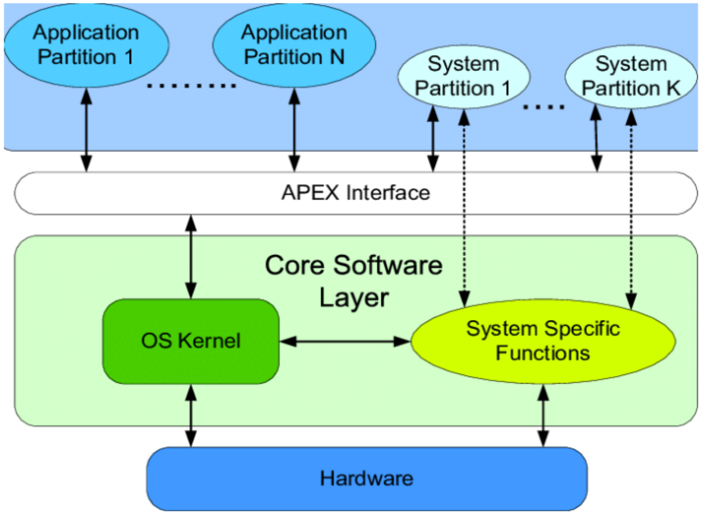
Acronym	Definition
App	Application
RTOS	Real Time Operating System
HW	Hardware

Figure 5. Configuration of an IMA System



What Worked and Didn’t Work; Benefits of Multi-Core Processors, ARINC 653 Architecture and MOSA?





Standard ARINC 653 Architecture

Results and Hope

Project SWAP reductions not based on Use of Open Software Standards such as FACE, etc.

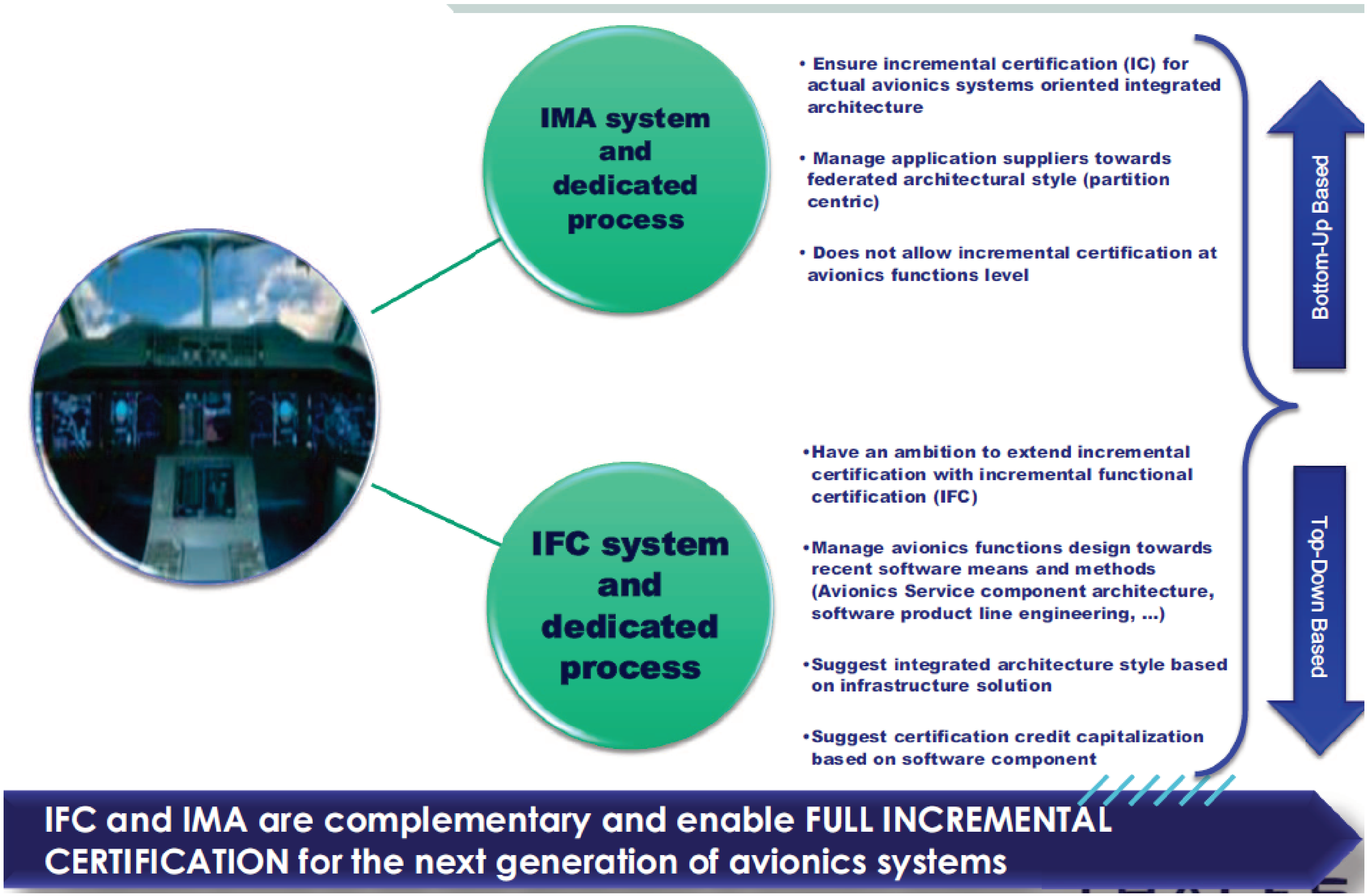
- JSF use of Simulation Based Acquisition (SBA) was a Failure; USAF had to take over Avionics Integration
- Civil Transport Aircraft, AB 380 & B787 developed Open IMA, e.g. IMA1G, Incremental Certification and Network robust partitioning worked
- Doubt if AADL, ACVIP, Digital Engineering, MBSE, SYSML etc. will have much impact on FVL, etc. **Hope MOSA can mature and help?**

Potential Benefits

Allow all cores to be used whatever the level of criticality

- Minimizes porting and re-certification efforts
- Compatibility with ARINC 663 and ARINC 664 guidelines for APEX and Network and Robust partitioning
- Incremental certification results in Space, Weight And Power (SWAP) Reduction and Cost Savings

Incremental Functional Certification for Avionics Functions Reuse & Evolution

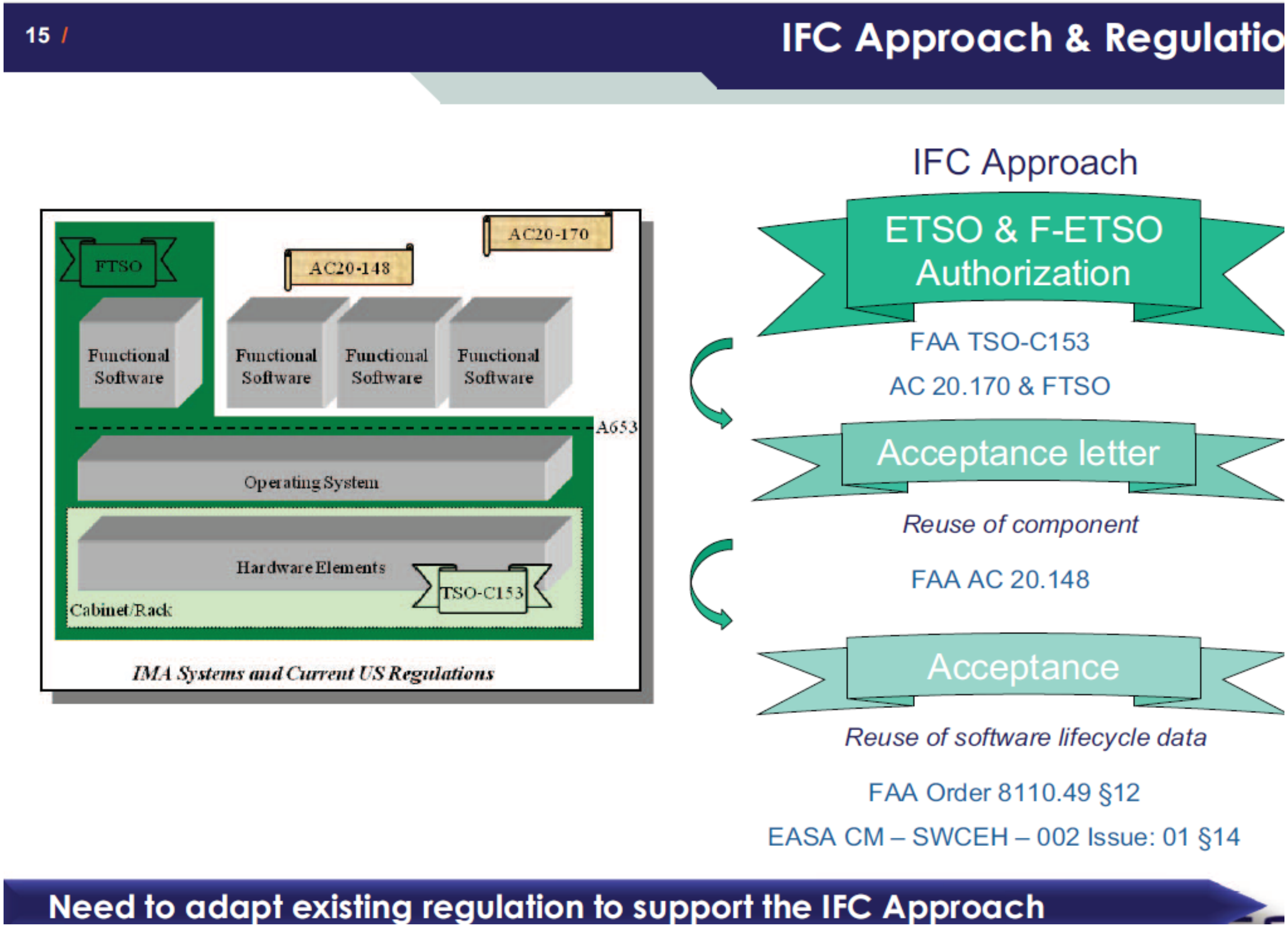

IMA system and dedicated process
IFC system and dedicated process
Bottom-Up Based
Top-Down Based

- Ensure incremental certification (IC) for actual avionics systems oriented integrated architecture
- Manage application suppliers towards federated architectural style (partition centric)
- Does not allow incremental certification at avionics functions level

- Have an ambition to extend incremental certification with incremental functional certification (IFC)
- Manage avionics functions design towards recent software means and methods (Avionics Service component architecture, software product line engineering, ...)
- Suggest integrated architecture style based on infrastructure solution
- Suggest certification credit capitalization based on software component

IFC and IMA are complementary and enable FULL INCREMENTAL CERTIFICATION for the next generation of avionics systems

Approved IFC for IMA Modules without Specific Aircraft Specification-Who is the Prime?



15 /

IFC Approach & Regulatio

IMA Systems and Current US Regulations

IFC Approach

ETSO & F-ETSO Authorization

FAA TSO-C153

AC 20.170 & FTSO

Acceptance letter

Reuse of component

FAA AC 20.148

Acceptance

Reuse of software lifecycle data

FAA Order 8110.49 §12

EASA CM – SWCEH – 002 Issue: 01 §14

Need to adapt existing regulation to support the IFC Approach

EASA initiated a new era of incremental certification for Integrated Modular Avionics
(21 Jun 2019)

- On June 18, 2019, the European Union Aviation Safety Agency (EASA) issued the first ETSO-2C153 certificate for an Integrated Modular Avionics (IMA) module to THALES AVS France SAS.
- With the ETSO-2C153 standard, together with the more recent ETSO-C214 for aircraft functions using an IMA platform, EASA is paving the way of the incremental certification in the domain of IMA.
- Equipment manufacturers can now obtain, independently from the aircraft TC process, incremental ETSO authorizations for their IMA platform and the ETSO functions that have been further developed on the certified IMA platform. Thanks to the pertinent requirements of the standards, the ETSO authorization brings a credit fully recognized at TC level and which reduces the TC certification effort
- FAA has followed with similar changes in an update of AC 20-170 IMA Guidelines to AC-20-170A in 2020 w/IFC guidance

EASA Has Recently Included a New IMC Certification Approach Providing a Coupling of ED-79 (ARP 4754°) with ED-124 (DO 297) and ED-12 (DO 178C) (ED Decision 2018/008/R Annex IV AMC 20-170, FAA Reluctant to Approve)

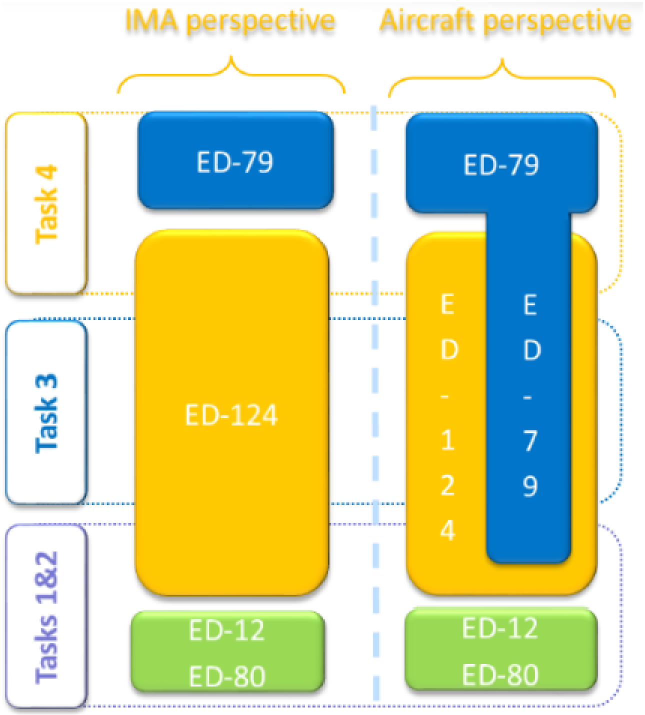


Figure 5 — Links between ED-124 tasks and other guidelines

Benefits

- Incremental Certification of a Component can take place w/o being part of an aircraft system
- Opens up certification to small Companies & suppliers
- FAA had some concern

- In order to maximize the credit taken from other standards and existing processes, two certification approaches based on the ED-124 tasks and objectives are considered eligible to support an IMA system certification:

(a)an IMA system perspective: by considering the application of ED-124 as a complete and consistent set of objectives;

(b) an aircraft perspective: where the IMA system certification and its specificities are addressed within the global framework of the aircraft certification and its related processes.

- This means that ED-124 considerations/objectives may be covered by other aircraft system processes and activities.
- ED-79 provides guidance and acceptable means of compliance for the development of systems, ED-79 processes may be used to cover ED-124 objectives and activities.
- However, the use of ED-79 will not ensure exhaustive coverage Of the ED-124 objectives. Consequently, the IMA-specific objectives and activities of ED-124 will remain to be addressed separately from the ED-79 objectives.

Benefits of Multi-Core Processors and ARINC 653 Architecture

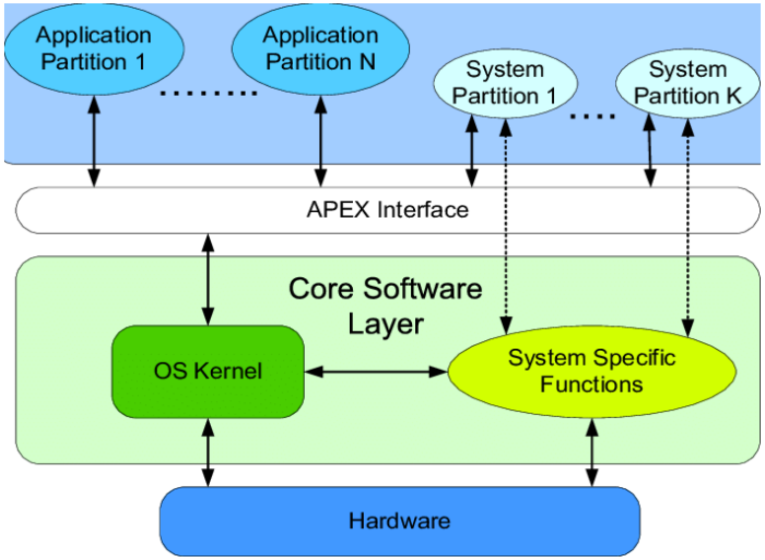
Benefits

Allow all cores to be used whatever the level of criticality

- Minimizes porting and re-certification efforts
- Compatibility with ARINC 663 and ARINC 664

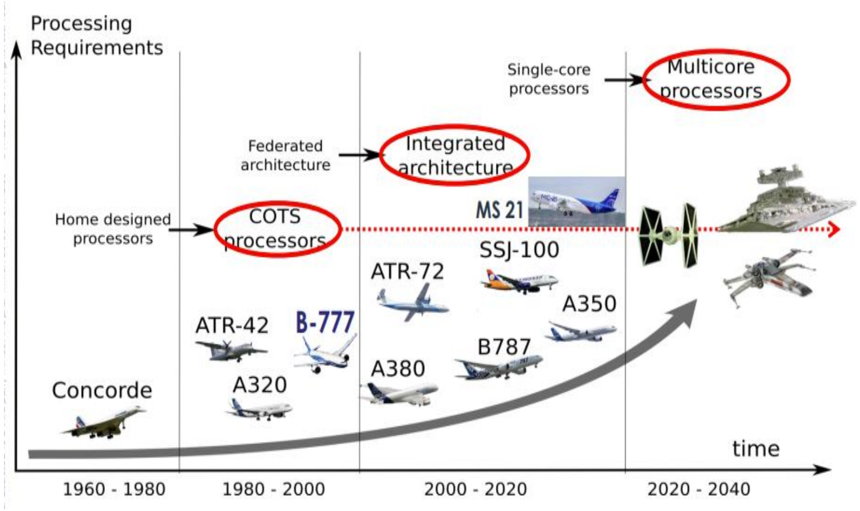
guidelines for Apex and Network partitioning

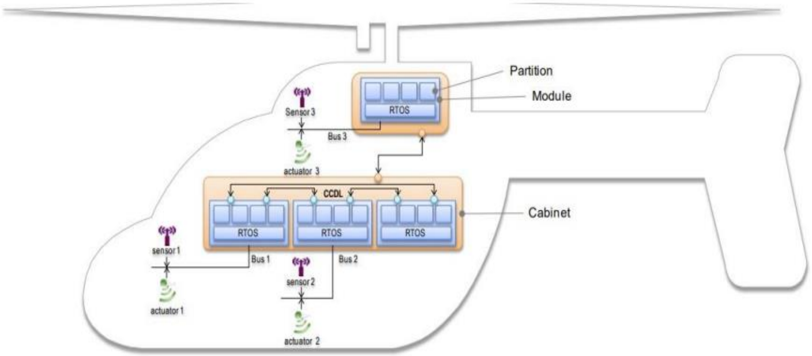
- Incremental certification



Standard ARINC 653 Architecture

Evolving Framework for Dynamic Reconfiguration and Run Time Assurance

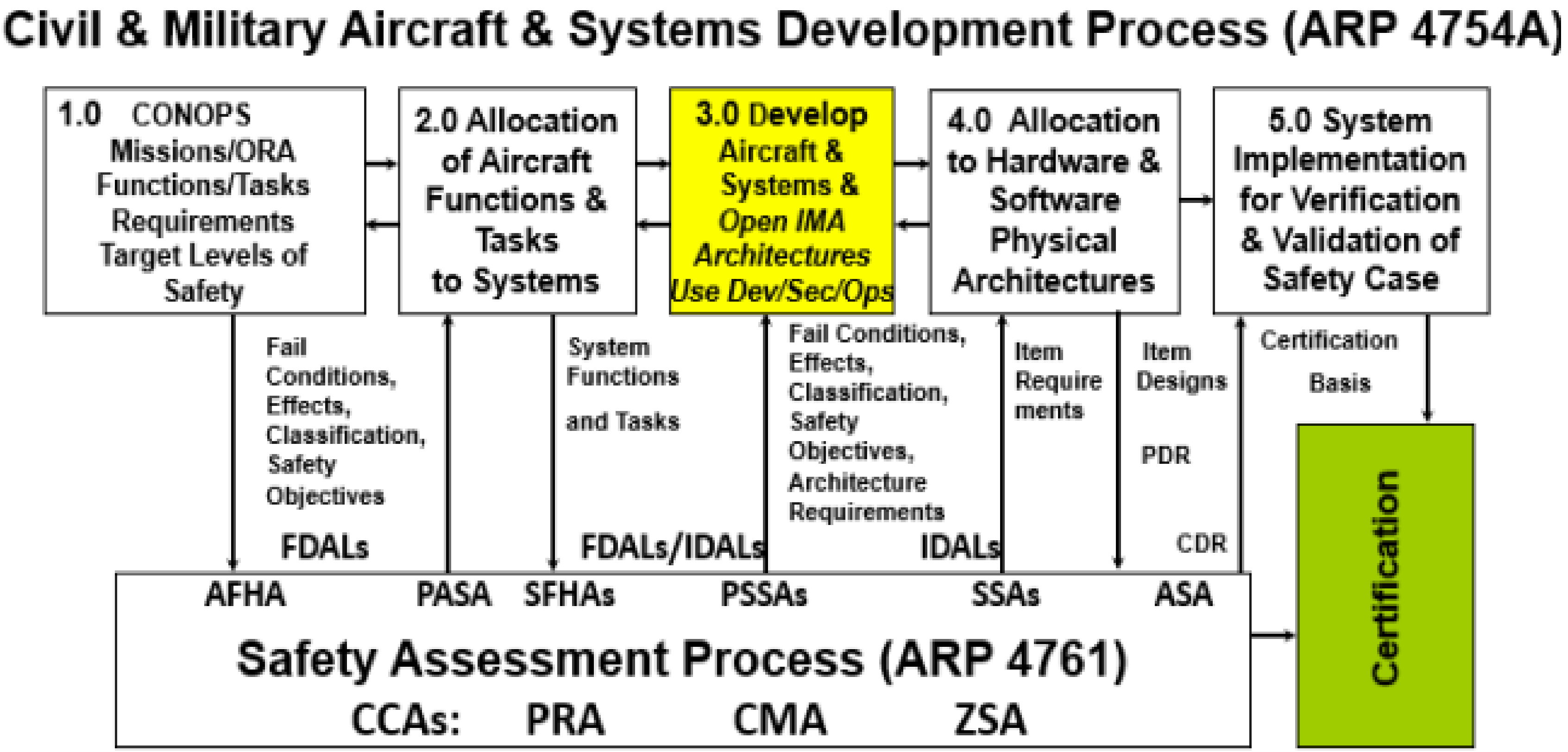




Evolution of MCPs in Civil Aircraft.

ARINC 653 IMA system architecture for Dynamic Reconfiguration

A Civil & Military Functional Safety Management (FSM) Development Assurance (DA) Open IMA Framework for Assured Autonomy for Air Vehicles



Civil & Military Aircraft & Systems Development Process (ARP 4754A)

1.0 CONOPS Missions/ORA Functions/Tasks Requirements Target Levels of Safety

2.0 Allocation of Aircraft Functions & Tasks to Systems

3.0 Develop Aircraft & Systems & *Open IMA Architectures Use Dev/Sec/Ops*

4.0 Allocation to Hardware & Software Physical Architectures

5.0 System Implementation for Verification & Validation of Safety Case

Fail Conditions, Effects, Classification, Safety Objectives

FDALs

System Functions and Tasks

FDALs/IDALs

Fail Conditions, Effects, Classification, Safety Objectives, Architecture Requirements

IDALs

Item Require ments

Item Designs

PDR

CDR

Certification Basis

Certification

AFHA PASA SFHAs PSSAs SSAs ASA

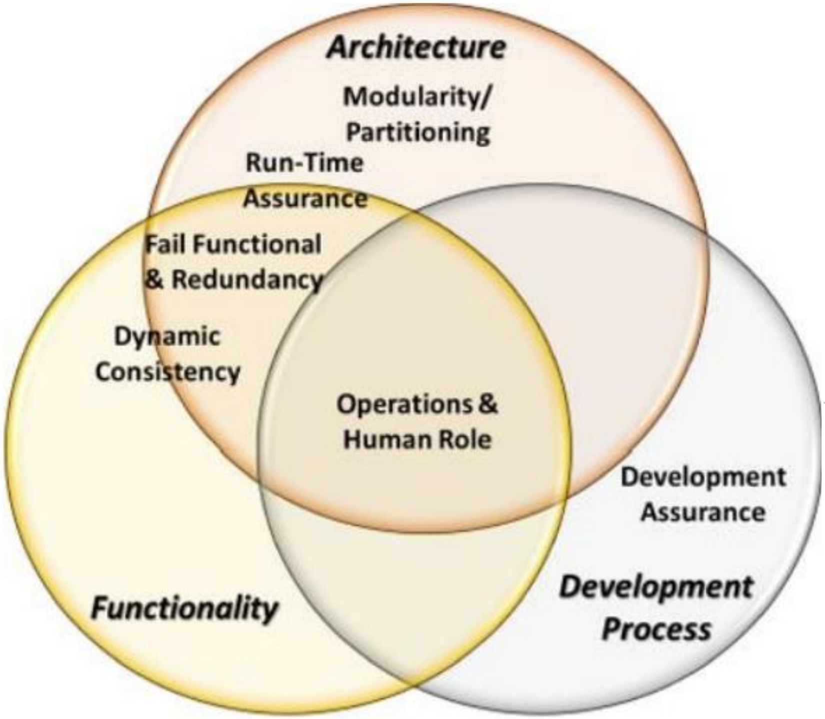
Safety Assessment Process (ARP 4761)

CCAs: PRA CMA ZSA

Development Assurance (DA) inherent in Framework

Design Time Assurance (DTA)	Run Time Assurance (RTA)
Reliability Based-MFOP Metric	Adaptive Reconfigurable Control
(Being Used in FARA Program)	(Being Demonstrated in Autonomy Prime)

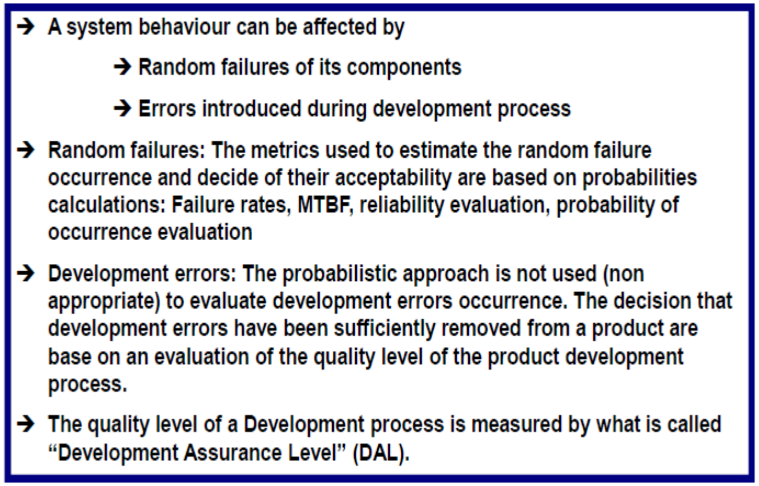
Identification of ASTM 377 Six Pillars of Autonomy and their Description for Insertion



- **Development Assurance:**: Techniques to gain safety assurance for complex systems as part of the development process.
- **Modularity and Partitioning:**: System architecture approaches that ensure that components can be developed and analyzed separately, while assuming a certain amount of independence from other unrelated functions (especially ones with differing criticality levels).
- **Operational Considerations and the Human Role**: All Automation systems must be considered in an operational context that includes the role of the human, including whether the system is assisting, augmenting, or replacing human decision-making.
- **Dynamic Consistency Checking**: Functionality that continuously checks data from sensors and algorithmic processing for logical consistency based upon a set of rules tied to established logical principles.
- **Fail Functional Design:** Design approaches—including redundancy—that ensure that even when failures occur, the system as a whole continues to function.
- **Run-Time Assurance**: Functional safety checks that monitor algorithm and system states in real time and, if necessary, trigger appropriate recovery(also known as safe'ing) behaviors.

What are Some Key Elements of Assured Autonomy

- **Development Assurance – Process and Error Based**
  - Inherent in the Civil Aircraft Development, Safety Assessment and Certification Framework as a Process Assessment
  - Assigns Development Assurance Levels (DALs) for Electronic Systems & Software in DO 178; Mechanical Systems and Hardware in DO 254
- **Design Time Assurance – Reliability & Random Failure Based**
  - Design approaches including redundancy can ensure that even when failures occur, the system as a whole continues to function.
  - Also can make use of Maintenance Free Operation Periods (MFOPs) as an alternative to MTBRs for sustaining Operational Availability (OA)



➔ A system behaviour can be affected by

➔ Random failures of its components

➔ Errors introduced during development process

➔ Random failures: The metrics used to estimate the random failure occurrence and decide of their acceptability are based on probabilities calculations: Failure rates, MTBF, reliability evaluation, probability of occurrence evaluation

➔ Development errors: The probabilistic approach is not used (non appropriate) to evaluate development errors occurrence. The decision that development errors have been sufficiently removed from a product are base on an evaluation of the quality level of the product development process.

➔ The quality level of a Development process is measured by what is called "Development Assurance Level" (DAL).

What are Assured Autonomy Key Elements?

- **Development Assurance (An Example of Aviation Implementation is shown in Figure 16)**
  - DA is included in ARP 4754A, DO 254 and DO 178 and defines development assurance as a process that "…establishes levels of confidence that development errors that can cause or contribute to identified failure conditions have been minimized with an appropriate level of rigor."
  - This historic development assurance guidance mandates the definition of intended function—a statement that the system will only do the right thing
- For Autonomy, it may be easier to prove the opposite—that the system will never do the wrong thing. Such a shift may seem subtle, but it is a large departure from the established approach to certification

Development Assurance

- Methodology
- UH-60M Description
- PASA
- PSSA
- FBW System
- Schematic Block Diagram
- FDAL Analysis
- Common Cause Analysis
- Abridged Petri Nets
- MFOP
- Conclusions

The Development Assurance Level assignment begins with Aircraft Functions and linking them to systems, subsystems, electronic hardware, and software.

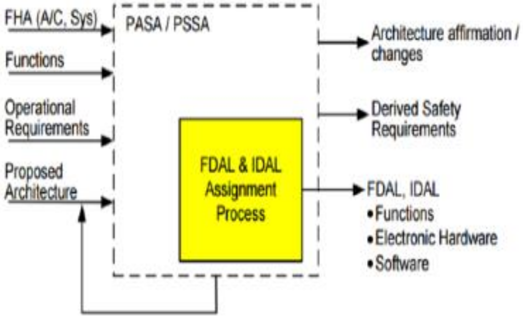
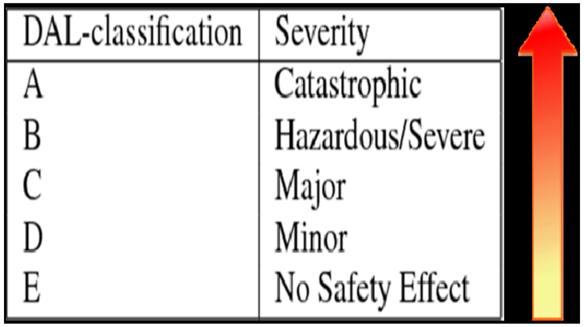


FIGURE 8 - FDAL/IDAL ASSIGNMENT PROCESS

TABLE 2 - TOP-LEVEL FUNCTION FDAL ASSIGNMENT

Top-Level Failure Condition Severity Classification	Associated Top-Level Function FDAL Assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E



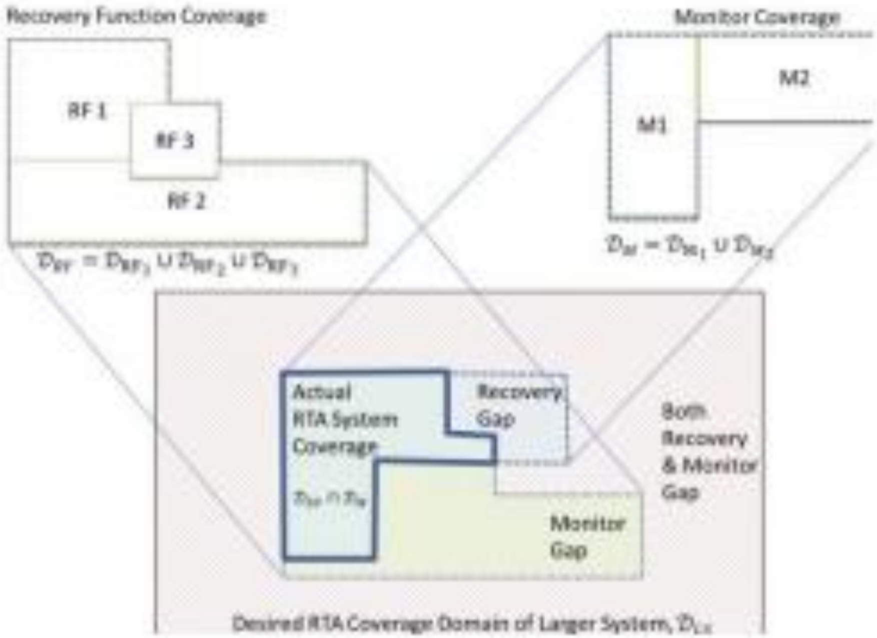
DAL-classification	Severity
A	Catastrophic
B	Hazardous/Severe
C	Major
D	Minor
E	No Safety Effect

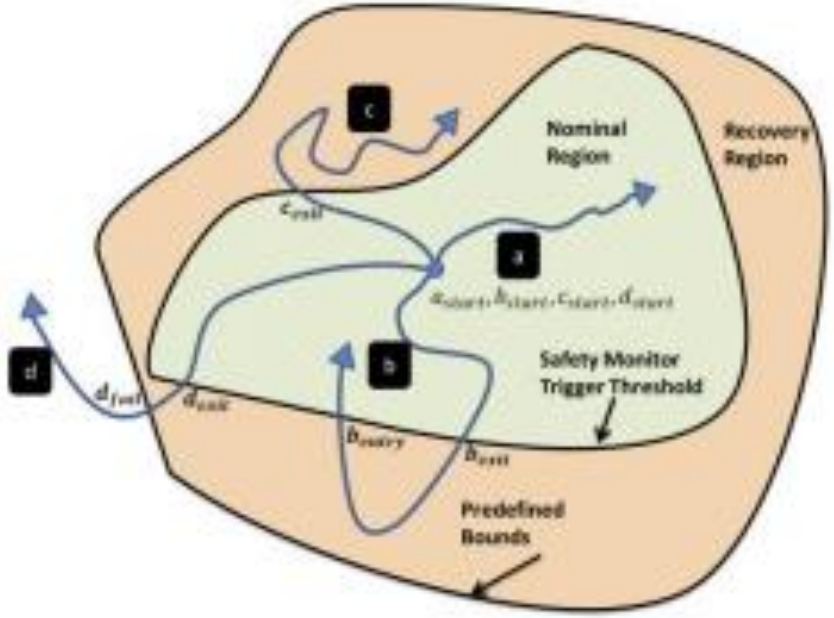
For **Catastrophic Failure Condition**, at least one development process is Level A, or at least two independent development processes are Level B, but no lower than level C (overall level A).

For **Hazardous Failure Condition**, at least one development process is Level B, or at least two independe development processes are Level C, and no lower than Level D (overall Level B).

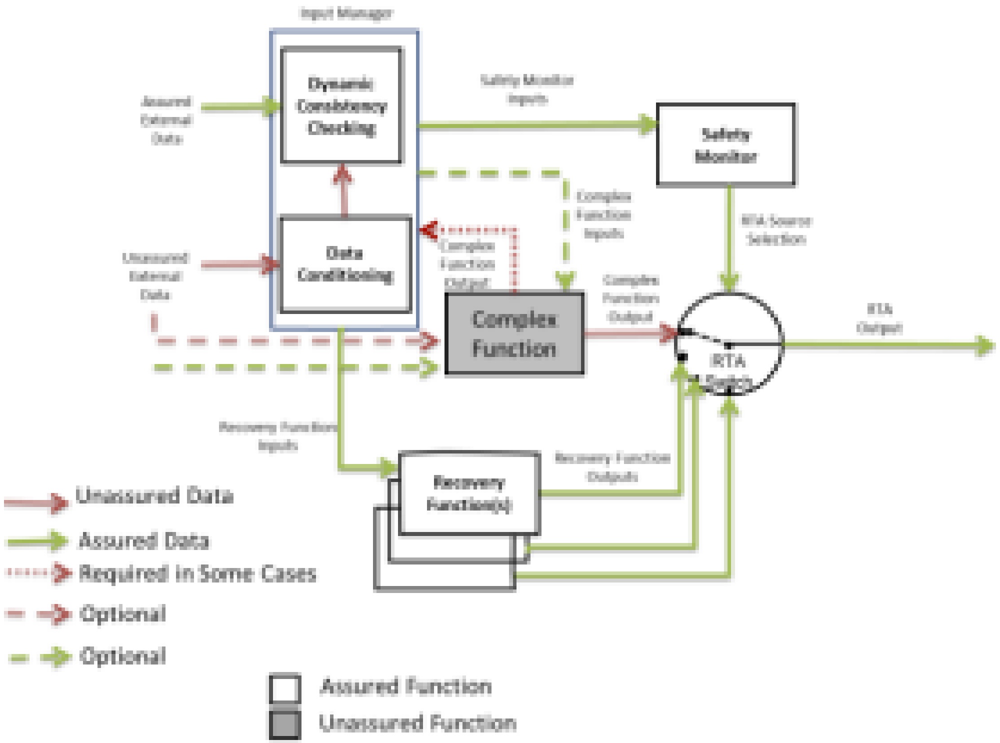
Once the DALs are assigned to items, they should be fed back to the system and aircraft processes to ensure that no common mode is inadvertently introduced that violates any claimed functional independence. **DALs are validated per System-level Safety Analysis and Component-Functional Failure Analysis**

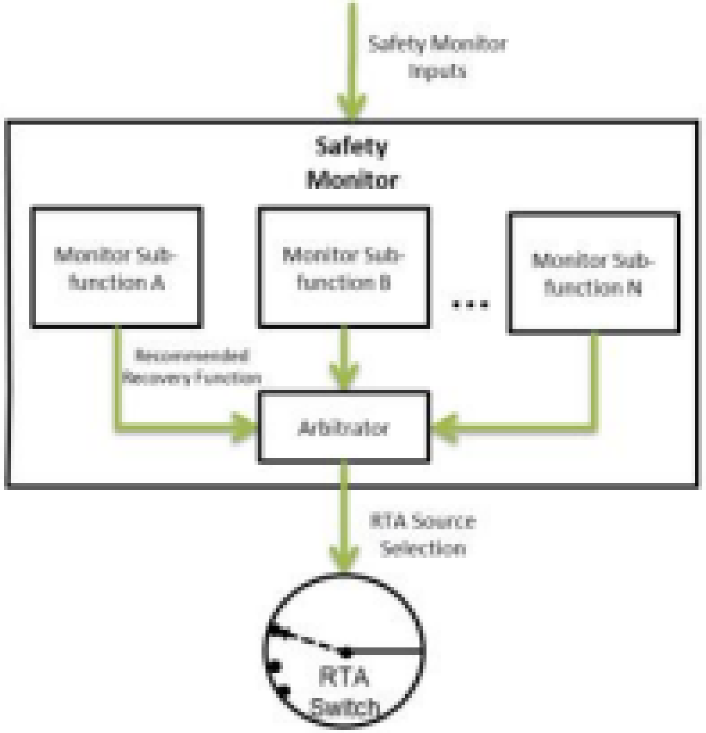
Run-Time Assurance System Coverage and RTA System Operational Scenario Example


Recovery Function Coverage
RF 1
RF 3
RF 2
$\mathcal{D}_{RF} = \mathcal{D}_{RF_1} \cup \mathcal{D}_{RF_2} \cup \mathcal{D}_{RF_3}$
Monitor Coverage
M1
M2
$\mathcal{D}_M = \mathcal{D}_{M_1} \cup \mathcal{D}_{M_2}$
Actual RTA System Coverage
$\mathcal{D}_{RF} \cap \mathcal{D}_M$
Recovery Gap
Both Recovery & Monitor Gap
Monitor Gap
Desired RTA Coverage Domain of Larger System, $\mathcal{D}_{LS}$

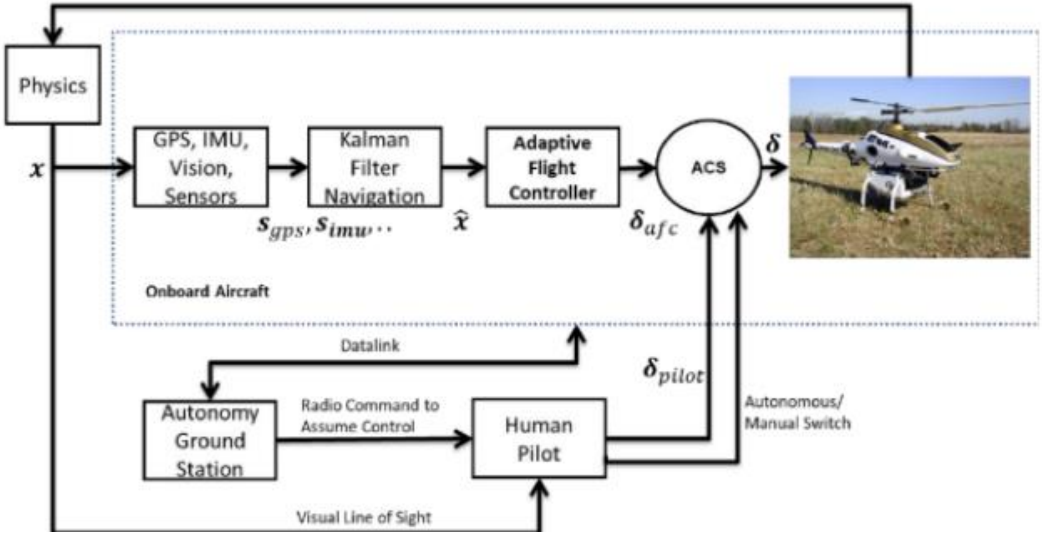


Run-Time Assurance Architecture and Multiple Monitoring Sub-Functions

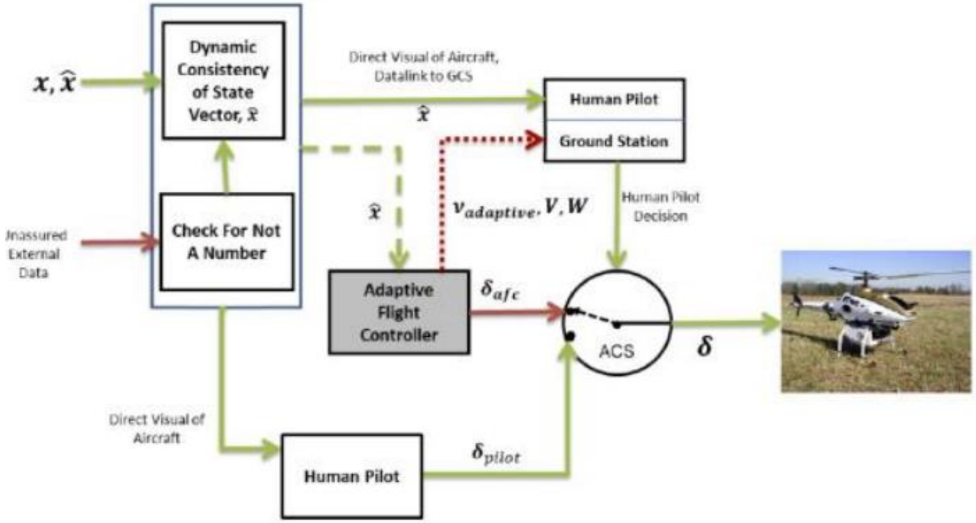




The physical architecture of components and Run ime Assurance for Adaptive Flight Controler that uses a Neural Network for Adaption w/Human pilot as the recovery function, e.g. Line of Sight

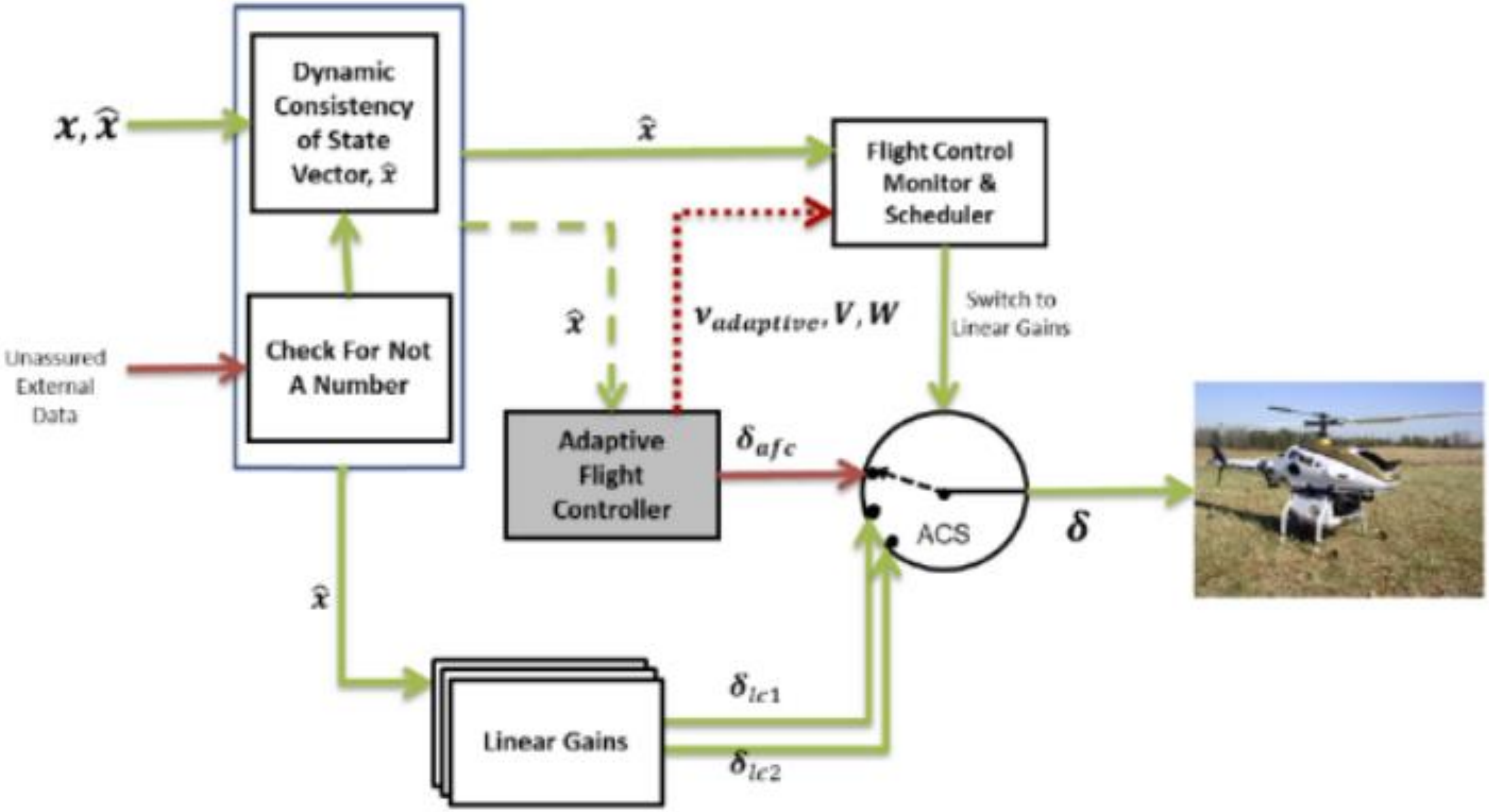


The physical architecture of components used to fly an experimental unmanned helicopter with a human safety pilot



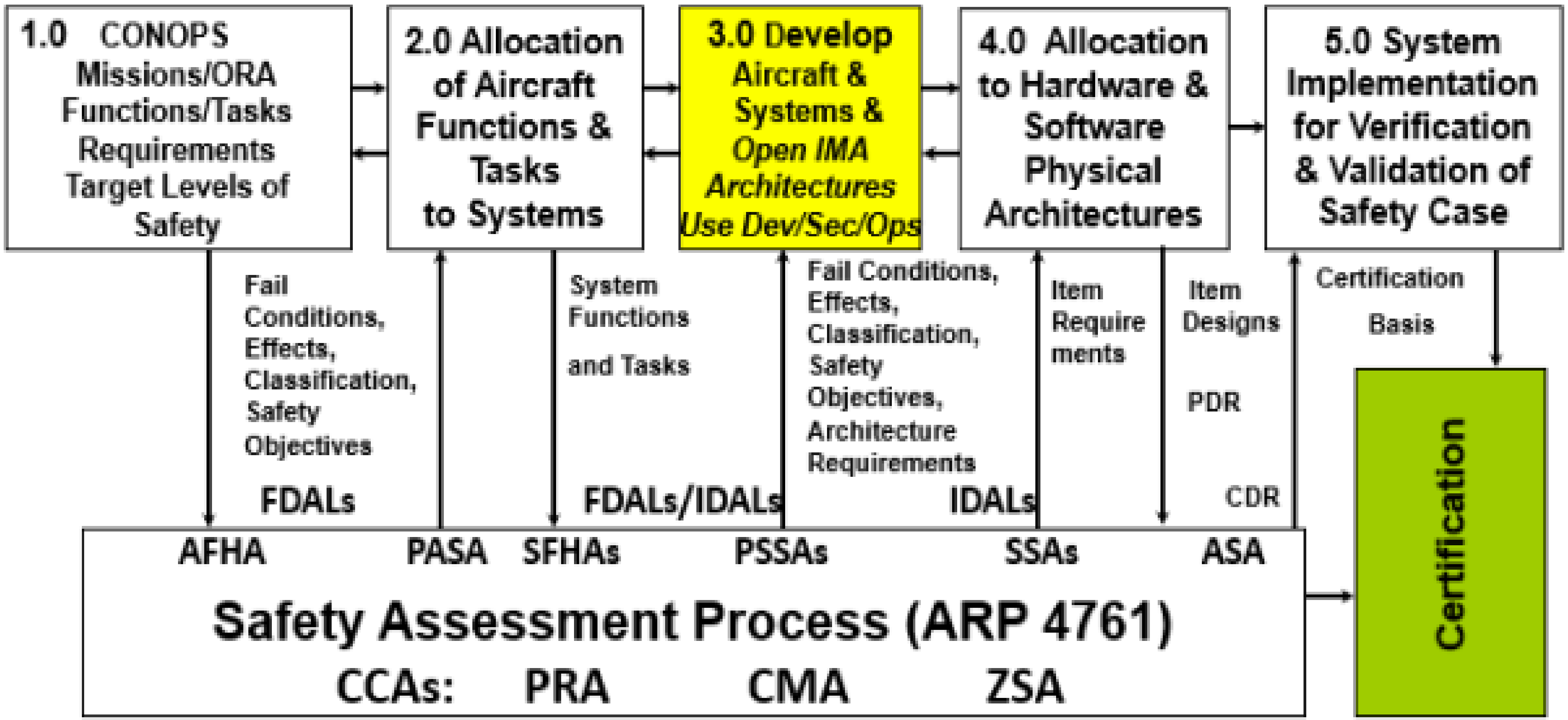
Run-Time Assurance based architecture for an Adaptive Flight Controller that uses a Neural Network for adaptation.
A human pilot acts as the recovery function.

: Run-Time Assurance based architecture for an Adaptive Flight Controller that uses a Neural Network for adaptation. No humans are available to act as a recovery function. Operation Beyond Line-of-Sight is Required.



A Civil & Military Functional Safety Management (FSM) Development Assurance (DA) Open IMA Framework for Assured Autonomy for Air Vehicles is Required

Civil & Military Aircraft & Systems Development Process (ARP 4754A)



1.0 CONOPS Missions/ORA Functions/Tasks Requirements Target Levels of Safety

2.0 Allocation of Aircraft Functions & Tasks to Systems

3.0 Develop Aircraft & Systems & *Open IMA Architectures Use Dev/Sec/Ops*

4.0 Allocation to Hardware & Software Physical Architectures

5.0 System Implementation for Verification & Validation of Safety Case

Fail Conditions, Effects, Classification, Safety Objectives

FDALs

System Functions and Tasks

FDALs/IDALs

Fail Conditions, Effects, Classification, Safety Objectives, Architecture Requirements

IDALs

Item Require ments

Item Designs

PDR

CDR

Certification Basis

AFHA PASA SFHAs PSSAs SSAs ASA

Safety Assessment Process (ARP 4761)

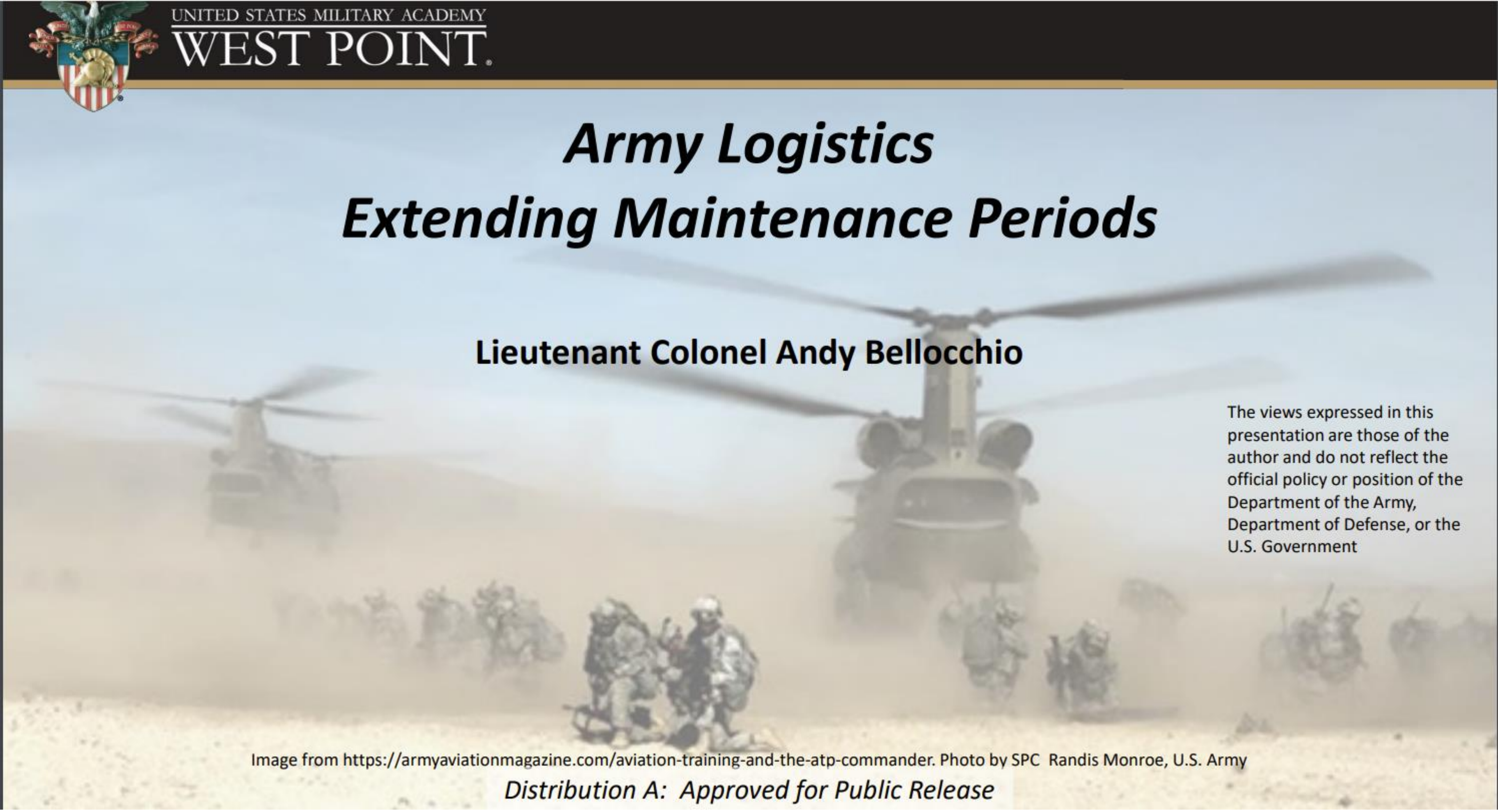
CCAs: PRA CMA ZSA

Certification

Conclusions and Recommendations

- AI Applications for Aviation Systems require a Systems Integration of Software and Hardware that only the DO 297/E 124 IMA can provide. FACE, etc. can contribute
- In addition, the robust partitioning, both spatial and temporal, inherent in an Open IMA with RTOS will be required to achieve the necessary safety capabilities for evolving Cyber Physical Vehicle Systems (CPVS) and necessary Adaptive Control
- The current coupling between ARP 4754A, DO 297 and DO 178C and 254 **is missing from the Military Approach**, AMACC. In 2018 EASA took steps to include it as an Acceptable Means of Compliance (AMC) in Annex IV of AMC 20-170; FAA has now followed with AC 20-170A: **Subject:** Integrated Modular Avionics (IMA), 2019
- Recommend this necessary coupling be included in the G-34 Committee AI Applications approach to eliminate the Gap between ARP 4754A and DO 178C, DO 254 and DO 297,
- Also, the Incremental Functional Certification (IFC) Approach in DO 297 is considered necessary for AI Applications and should be included.

MFOP Approach for FARA



UNITED STATES MILITARY ACADEMY
WEST POINT.

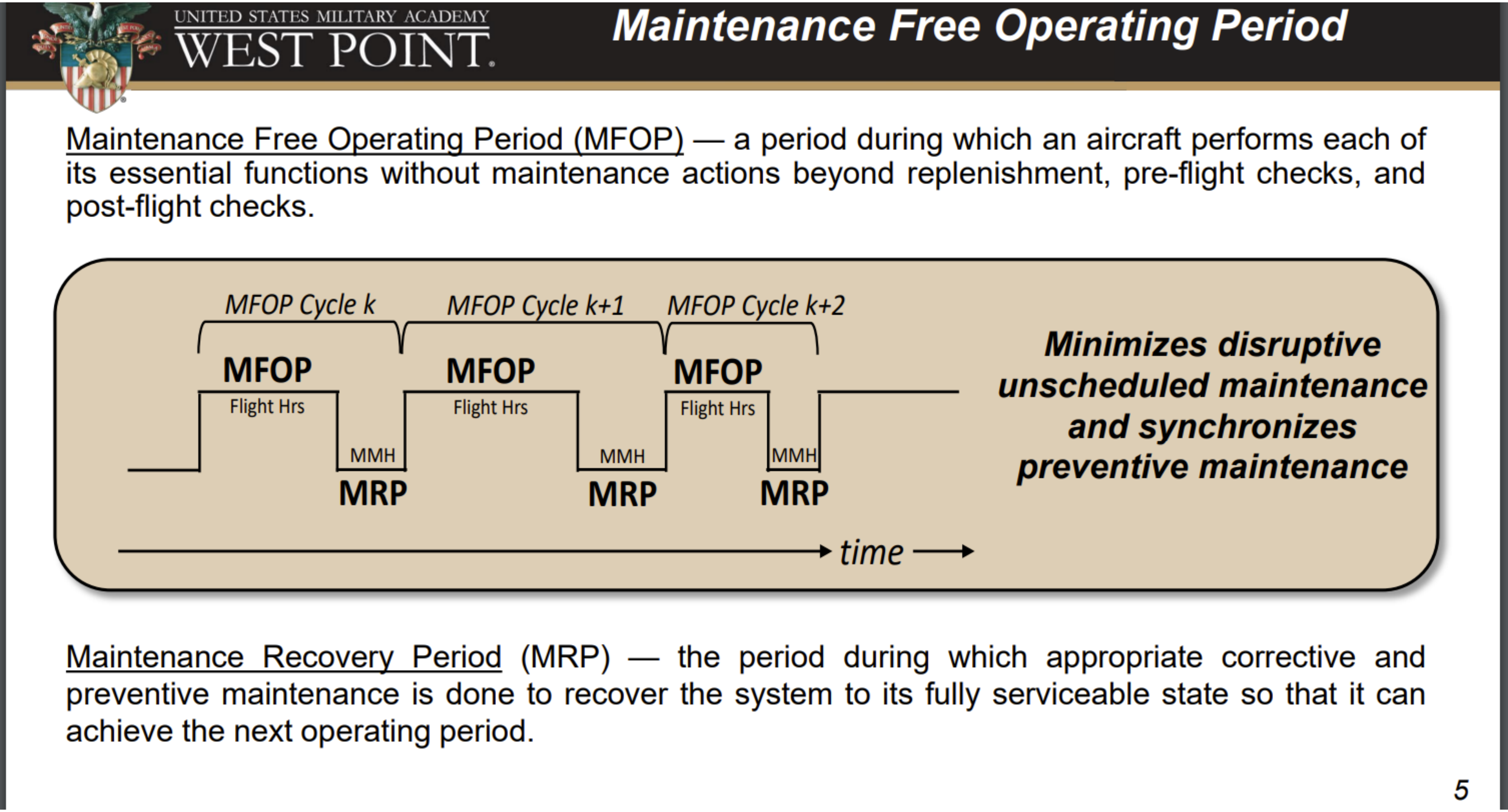
Army Logistics
Extending Maintenance Periods

Lieutenant Colonel Andy Bellocchio

The views expressed in this presentation are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government

Image from https://armyaviationmagazine.com/aviation-training-and-the-atp-commander. Photo by SPC Randis Monroe, U.S. Army

Distribution A: Approved for Public Release



UNITED STATES MILITARY ACADEMY
WEST POINT.

Maintenance Free Operating Period

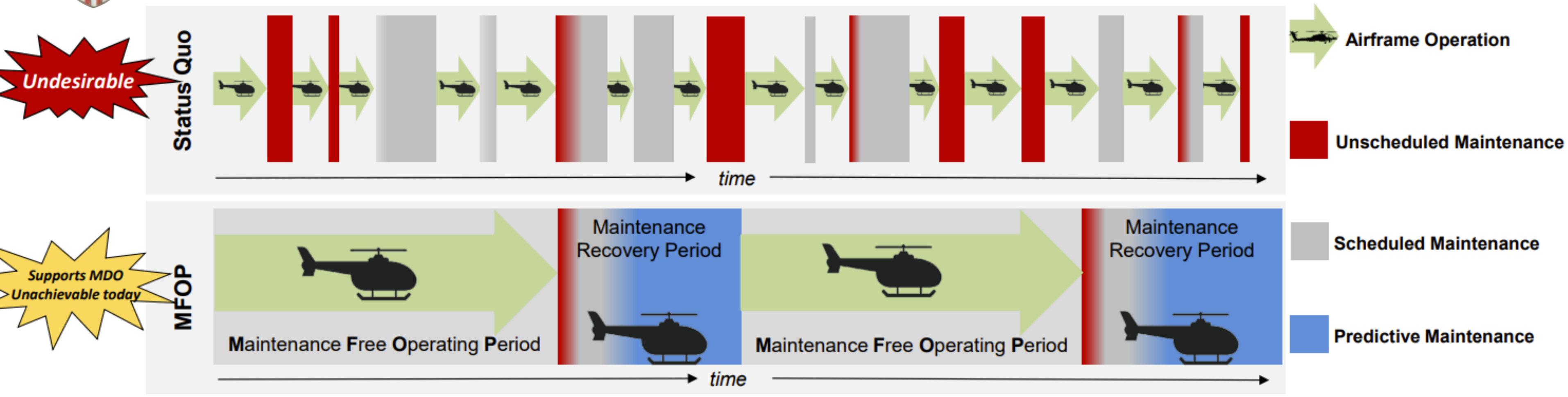
Maintenance Free Operating Period (MFOP) — a period during which an aircraft performs each of its essential functions without maintenance actions beyond replenishment, pre-flight checks, and post-flight checks.

MFOP Cycle k
MFOP Cycle k+1
MFOP Cycle k+2
MFOP
Flight Hrs
MMH
MRP
MFOP
Flight Hrs
MMH
MRP
MFOP
Flight Hrs
MMH
MRP
time

Minimizes disruptive unscheduled maintenance and synchronizes preventive maintenance

Maintenance Recovery Period (MRP) — the period during which appropriate corrective and preventive maintenance is done to recover the system to its fully serviceable state so that it can achieve the next operating period.

Using MFOP to improve disbursed operations



TRADOC Pamphlet 525-3-1 [12] states that to prevail in competition during MDO, FVL must:

- Conduct independent maneuver to penetrate strategic and operational standoff
- Sustain and protect organic assets until the MDO formation can regain contact with adjacent or supporting units
- **Operate with a reduced logistics demand to maintain offensive operations for 72-96 hours**
- Employ split basing between operational support and tactical support areas

Jaunt Air Mobility Functional Safety Management Open IMA Approach for System Safety Assessment and Certification

Dr. Daniel P. Schrage
Former System Safety Lead, Jaunt Air Mobility
Professor Emeritus, School of AE, Georgia Tech
Member, SAE S-18 Safety Assessment and Certification Committee
Member, SAE G-34 AI for Applied Aviation Systems Committee