Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

Integrated Modular Avionics
Development Guidance and Certification Considerations

René L.C. Eveleens
National Aerospace Laboratory NLR
P.O. Box 90502
1006BM Amsterdam

RTO SCI LS-176: “Mission System Engineering”
November 2006

IMA Certification Guidance

introduction to avionics certification processes

certification guidance

EUROCAE WG60 background

the definition of IMA

goal of the guidance document

the concept of "incremental acceptance"

IMA certification guidance document

conclusion

System verification (1/2)

differences / similarities with "normal testing"?

- main difference
  certification by an independent third party:
  certification authority

- other differences / similarities basically depend on your development and testing maturity...

- no requirements means: testing in the dark!

System verification (2/2)

verification according to RTCA DO-178

- "… the evaluation of the results of a process to ensure correctness and consistency with respect to the inputs and standards to that process."

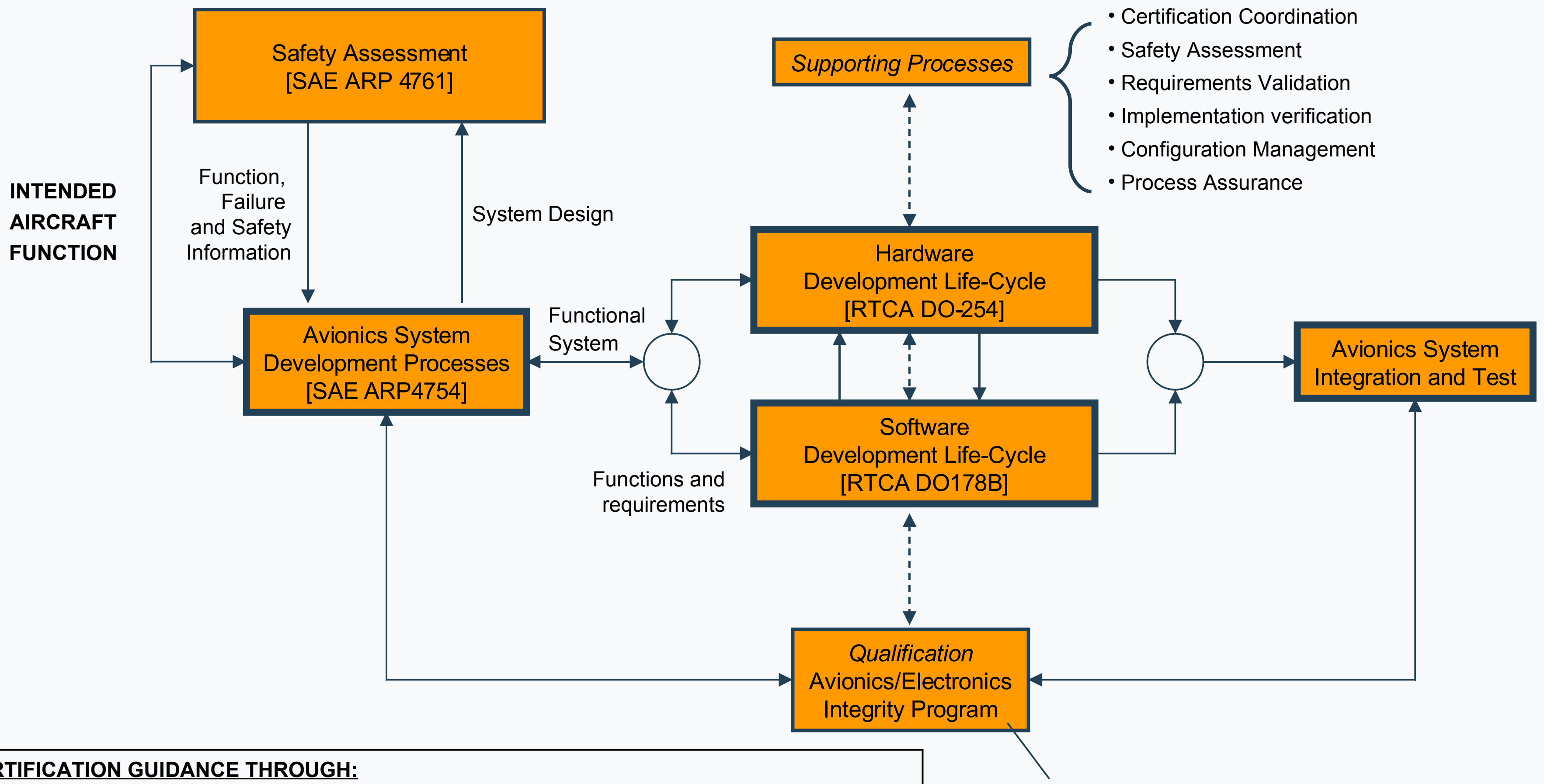
testing according to RTCA DO-178

- ″… the process of exercising a system or system component to verify that it satisfies specified requirements and to detect errors."

but

- testing cannot show the absence of errors
- therefore extensive verification effort required
  - requirements analysis and traceability
  - consistent documentation

Certification processes



- Certification Coordination
- Safety Assessment
- Requirements Validation
- Implementation verification
- Configuration Management
- Process Assurance

CERTIFICATION GUIDANCE THROUGH:

SAE ARP 4754 Certification considerations for highly-integrated or complex aircraft systems

SAE ARP 4761 Safety Assessment Process Guidelines & Methods

RTCA DO-178B Software Considerations in Airborne Systems and Equipment Certification

RTCA DO-254 EUROCAE ED-80 Design Assurance Guidance for Airborne Electronic Hardware

RTCA DO-160D Environmental Test Specifications

MIL-HDBK-87244 (USAF) Avionics/Electronics Integrity

- Concept Exploration
- Demonstration/Validation
- Engineering/Manufacturing Development
- Production
- Operation & Support

DO-178B overview: introduction

Not a development standard: a guideline for certification

Emphasis on requirements-based development

Emphasis on verification/testing

Based on a system safety assessment, software is assigned a safety criticality level

Safety according to DO-178B: increasing verification/testing effort with increasing software levels

Software criticality levels

Software Level	**Aircraft level Criticality**	**Meaning**
A	Catastrophic	Aircraft destroyed, Many fatalities
B	Hazardous	Damage to aircraft, Crew overextended, Occupants hurt, some fatal
C	Major	Large reduction in safety margins, occupants injury
D	Minor	Little effect on operation of aircraft and crew workload
E	No effect	No effect on operation of aircraft or crew workload

Life cycle processes

Software planning process (1 table with process objectives and outputs by software level)

Software development processes (1 table)

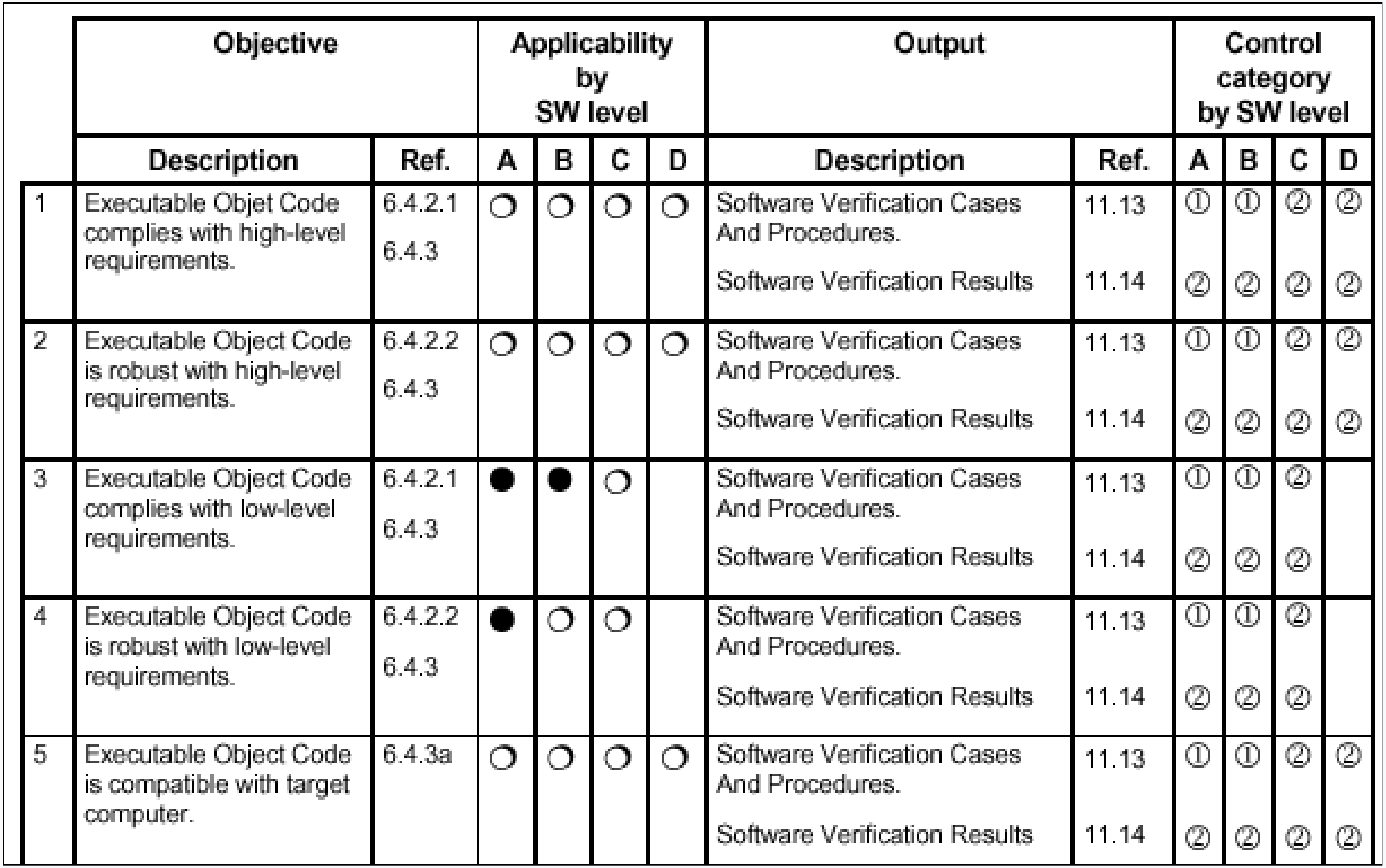
Software verification processes (5 tables) [next slide]

Software configuration management process (1 table)

Software quality assurance process (1 table)

Certification liaison process (1 table)

Objective tables (example)



	Objective		Applicability by SW level				Output		Control category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Executable Objet Code complies with high-level requirements.	6.4.2.1 6.4.3	○	○	○	○	Software Verification Cases And Procedures. Software Verification Results	11.13 11.14	① ②	① ②	② ②	② ②
2	Executable Object Code is robust with high-level requirements.	6.4.2.2 6.4.3	○	○	○	○	Software Verification Cases And Procedures. Software Verification Results	11.13 11.14	① ②	① ②	② ②	② ②
3	Executable Object Code complies with low-level requirements.	6.4.2.1 6.4.3	●	●	○		Software Verification Cases And Procedures. Software Verification Results	11.13 11.14	① ②	① ②	② ②	
4	Executable Object Code is robust with low-level requirements.	6.4.2.2 6.4.3	●	○	○		Software Verification Cases And Procedures. Software Verification Results	11.13 11.14	① ②	① ②	② ②	
5	Executable Object Code is compatible with target computer.	6.4.3a	○	○	○	○	Software Verification Cases And Procedures. Software Verification Results	11.13 11.14	① ②	① ②	② ②	② ②

Certification guidance

Software Lifecycle Data Items

Plan for Sw Aspects of Cert. (PSAC)

Software Dev. Plan

Software Ver. Plan

Software CM Plan

Software QA Plan

Software Rqmts Stnds

Software Design Stnds

Software Code Stnds

Software Rqmts Data

Design Description

Source Code

Executable Object Code

Software Ver Cases and Procs

Software Verification Results

Software LifeCycle Environment

Configuration Index

Software Configuration Index

Problem Reports

Software CM Records

Software Quality Assurance Records

SW Accomplishments Summary

The DO-178B verification/testing process: (global) specification

Level E: no activities (DO-178B not applicable)

Level D: test coverage of high-level requirements

Level C: level D +

- test coverage of low-level requirements +
- structural coverage: 100 % statement coverage

Level B: level C +

- structural coverage: 100 % decision coverage

Level A: level B +

- structural coverage: 100 % modified condition/decision coverage, based on object code

WG60/SC200 background - facts

EUROCAE WG60 (start: Sept 2001)

title: “Integrated Modular Avionics” (IMA)

joined with RTCA SC-200 (Nov 2002)

chairmen and secretaries

- WG60 co-chair: René Eveleens (NLR)
- WG60 co-secretary: David Brown (Airbus UK)
- SC200 co-chair: Cary Spitzer (Avionicon)
- SC200 co-secretary: John Lewis (FAA)

WG60/SC200 background - mission

propose, document and deliver means to support the certification (or approval) of modular avionics, systems integration, and hosted applications, including considerations for installation and continued airworthiness in all categories and classes of aircraft

WG60/SC200 background
- terms of reference

modular avionics

- define key characteristics
- specific issues in regulatory materials and practices
- stand-alone approval
- re-use of accepted process, data, product, etc.
- safety and performance issues
- involvement of certification authorities
- support TSO, AC, ACJ production
- close working relationship with other groups

other topics

- fault management and health monitoring, safety, environmental qualification, configuration management, development assurance, incremental qualification, single-event-upset, electrical systems, etc.

WG60/SC200 background - participants

wide participation

- industry (avionics and aircraft integrators)
- certification authorities
- research establishments

overview of companies involved

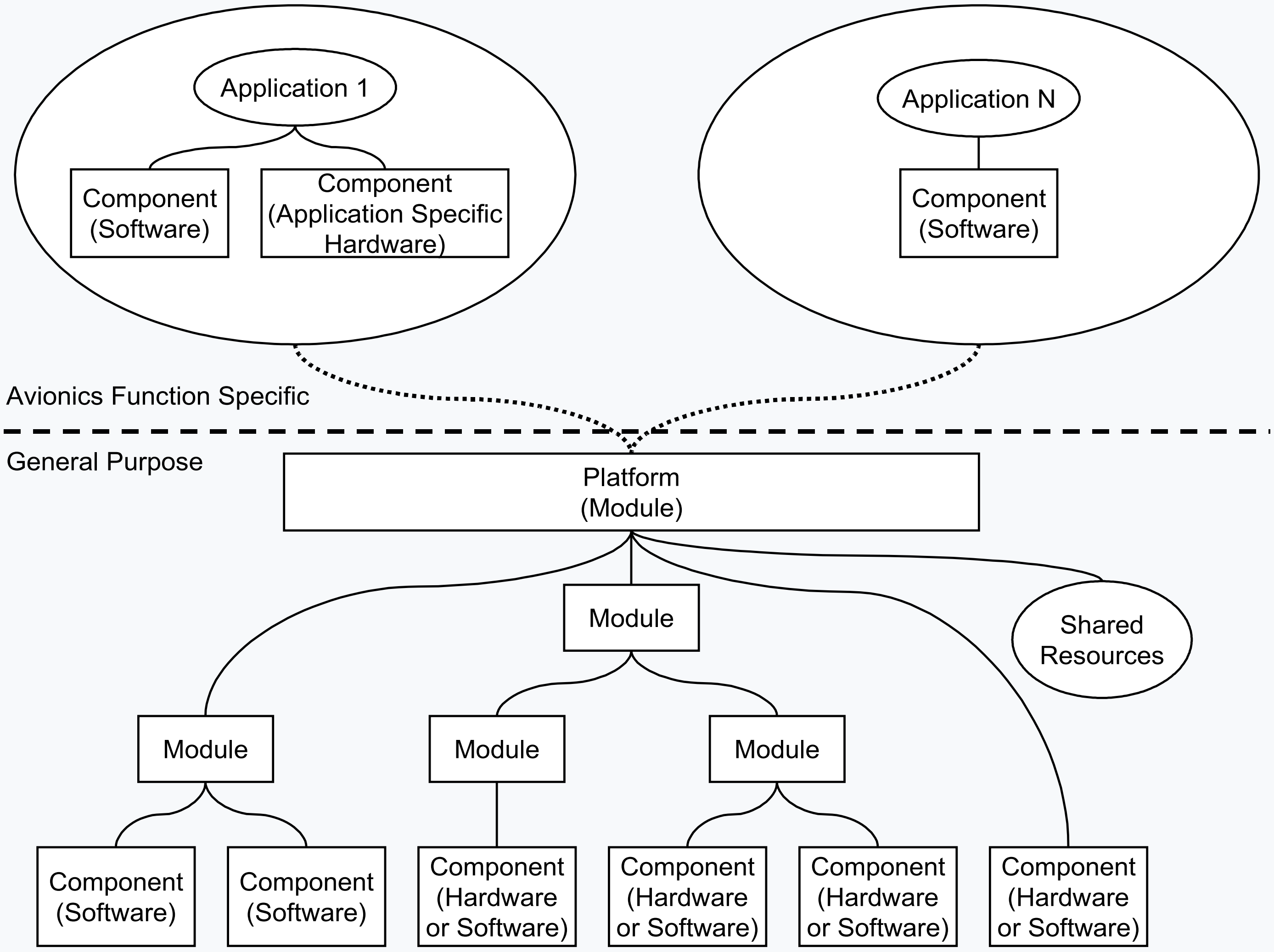
- FAA, CAA, DGAC, Airbus, Boeing, Honeywell, NASA, ARINC, Thales, Rockwell Collins, Diehl, Smiths Aerospace, Transport Canada, BAE Systems, NLR, TTTech, Pilatus etc.

WG60/SC200 background - status

IMA development guidance and certification considerations

- RTCA issued DO-297
- EUROCAE planned to issue ED-124

the definition of IMA - terminology


Application 1
Component (Software)
Component (Application Specific Hardware)
Application N
Component (Software)
Avionics Function Specific
General Purpose
Platform (Module)
Module
Shared Resources
Module
Module
Module
Component (Software)
Component (Software)
Component (Hardware or Software)
Component (Hardware or Software)
Component (Hardware or Software)
Component (Hardware or Software)

the definition of IMA - periphery

goal

- availability
- integrity
- safety
- health monitoring and fault management
- composability

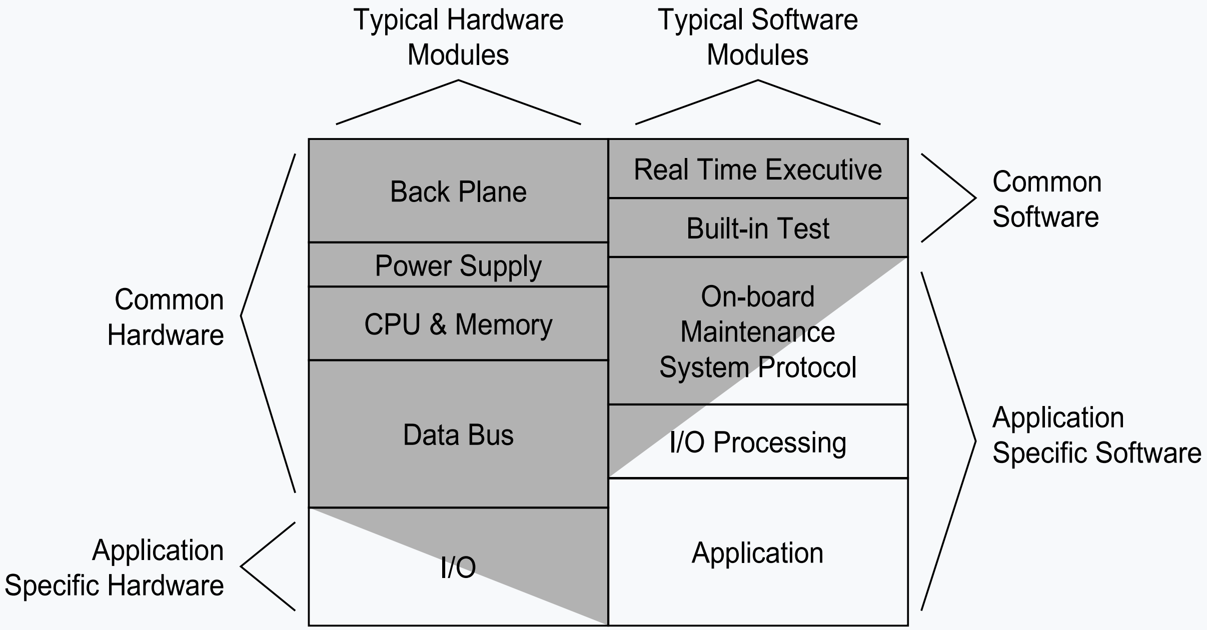
stakeholders

- certification authorities
- certification applicant
- IMA system integrator
- platform and module suppliers
- application suppliers
- maintenance organization

the definition of IMA - characteristics

key characteristics

- platform and hosted applications
- shared resources
- robust partitioning
- application programming interface (API)
- health monitoring and fault management



Typical Hardware Modules

Typical Software Modules

Back Plane

Power Supply

CPU & Memory

Data Bus

I/O

Real Time Executive

Built-in Test

On-board Maintenance System Protocol

I/O Processing

Application

Common Hardware

Application Specific Hardware

Common Software

Application Specific Software

goal of the guidance document

quote WG60/SC200 mission:

“support the certification (or approval) of modular avionics, systems integration, and hosted applications, including considerations for installation and continued airworthiness in all categories and classes of aircraft”

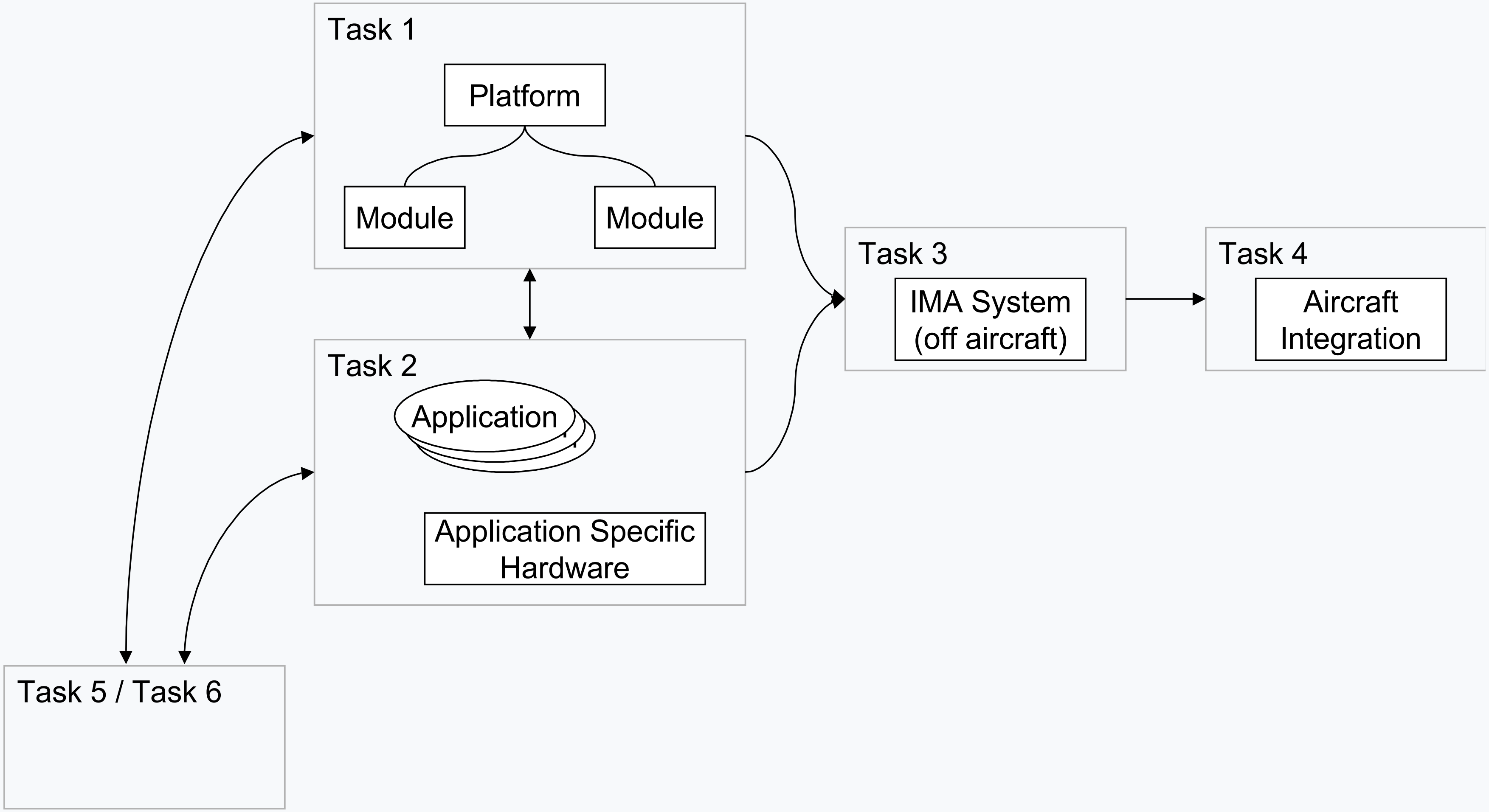
the concept of "incremental acceptance"

definition

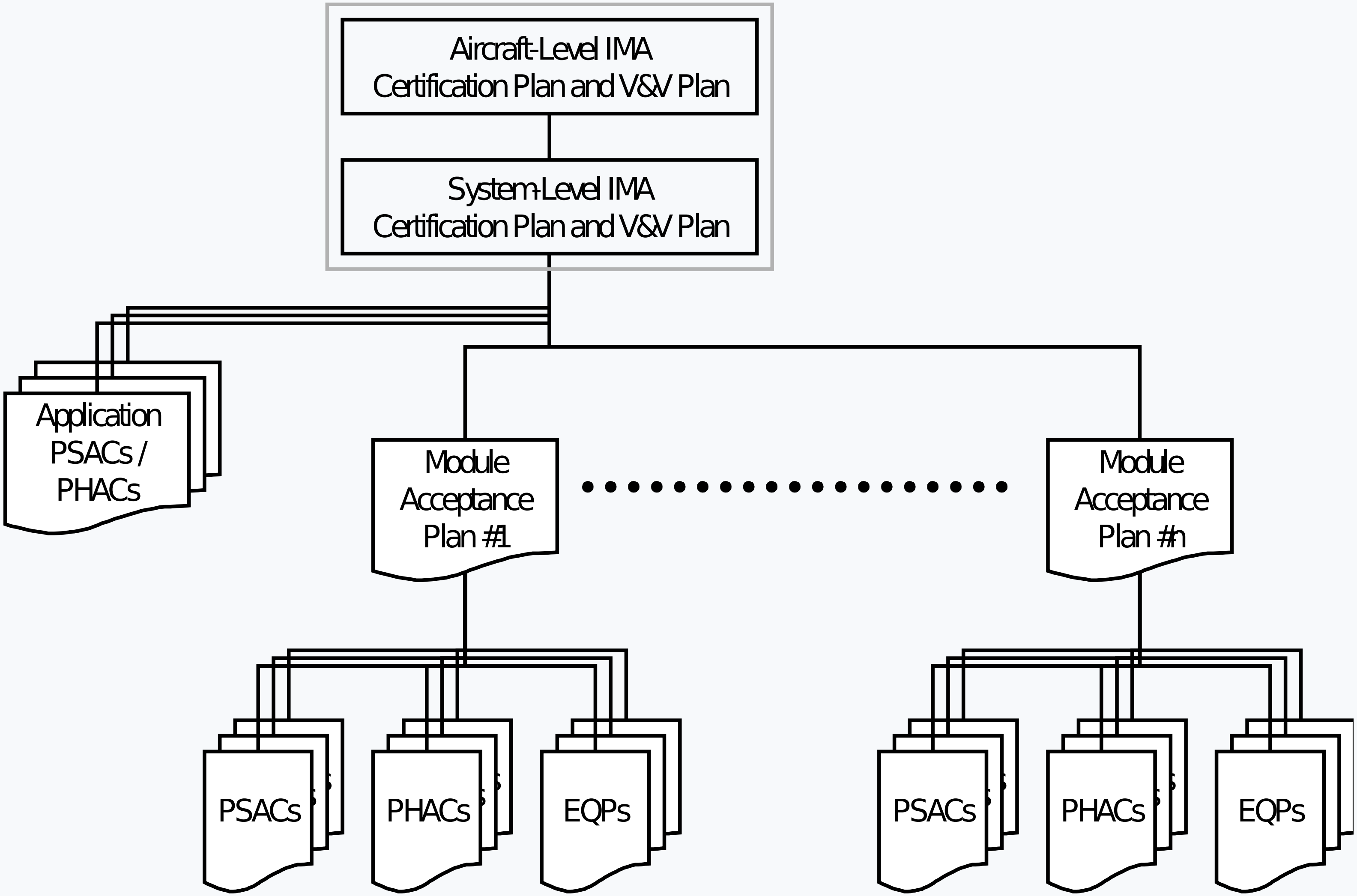
- a process for obtaining credit toward approval and certification by accepting or finding that an IMA module, application, and/or off-aircraft IMA system complies with specific requirements. Credit granted for individual tasks contributes to the overall certification goal

Integration Activity	Acceptance Tasks	
Integrate components and/or modules to form a platform	Task 1	Module and/or platform acceptance
Integrate a single application with the platform	Task 2	Application acceptance (software and/or hardware)
Integrate multiple applications with the platform(s) and one another	Task 3	IMA system acceptance
Integrate IMA system with aircraft and its systems	Task 4	Aircraft integration
Identify changes and their impacts, and need for re-verification	Task 5	Change
Identify and use IMA components on other IMA systems and installations	Task 6	Reuse

IMA guidance document - certification tasks



IMA guidance document
- certification data



IMA guidance document
- objective tables

example:

- IMA platform development process objectives

ID	Objective Summary	Doc ref	Life Cycle Data Description	Life Cycle Data Reference	Control Category
1	Failure reporting process is defined and in place to support continued airworthiness requirements for IMA system components which may be used in more that one IMA system.	3.6	Aircraft Instructions for Continued Airworthiness and/or IMA System Certification Plan (or other lower level component's plan)	ICAW	CC1

conclusion

IMA certification considerations

- document jointly prepared by RTCA / EUROCAE
- DO-297 / ED-124
- incremental acceptance
- guidance on
  - definition of IMA
  - design considerations
  - certification tasks
- broad scope of stakeholders
- wide acceptance
  - industry
  - certification authorities