Integrated Modular Avionics
Development Guidance and Certification Considerations

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

eveleens@nlr.nl

ABSTRACT

From 2001 to 2005 a working group within the European Organisation for Civil Aviation Equipment (EUROCAE) has been working on the definition of development guidance and certification considerations for Integrated Modular Avionics. This paper explains the standardised terminology, the concept of incremental acceptance, the certification tasks and associated certification data and the many objectives defined in this guidance document, which will be published in 2006 as ED-124.

1.0 INTRODUCTION

The use of Integrated Modular Avionics (IMA) is rapidly expanding and is found in all classes of aircraft. In recognition of this rapid growth RTCA established Special Committee 200 (SC-200) and EUROCAE established Working Group 60 (WG-60) to jointly develop a document that could be used as guidance in the design, development and application of IMA. This paper explains the background of this document, introduced the terminology and processes required for a smooth certification process of IMA.

2.0 BACKGROUND

At the start of this century, within the avionics industry it was felt that there was a urgent need for guidance on development processes and certification issues for modular avionics. The modular avionics technology had come to a maturity level and industry was now ready to bring products to the market. Biggest challenge within this area is that modular avionics is a composition of building blocks, preferably supplied by different companies in the supply chain. Each supplier is supposed to bring its part to a certain level of qualification, and after this a system integrator can use these "pre-qualified" part in the overall certification process.

To face this challenge EUROCAE founded a working group (number 60) in September 2001, which was tasked to define this guidance. Later, in November 2002, there was a merge with an RTCA steering committee (number 200). The mission of this joint working group was to "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".

Besides this mission, the term of reference for both WG60 and SC200 stated that the group would define key characteristics of modular avionics, define specific issues in regulatory materials and practices, aims

Eveleens, R.L.C. (2006) Integrated Modular Avionics Development Guidance and Certification Considerations. In *Mission Systems Engineering* (pp. 4-1 – 4-18). Educational Notes RTO-EN-SCI-176, Paper 4. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int.

for stand-alone approval of individual building blocks, assure the re-use of accepted process, data, product, etc., tackle safety and performance issues, involve certification authorities and support TSO, AC, ACJ production, and have a close working relationship with other groups.

During its existence the group has had a wide participation from industry (both avionics industry and aircraft integrators), certification authorities and research establishments. The final document was delivered end of 2005. RTCA has issued the document as DO-297. EUROCAE is planning to issue the document in 2006 as ED-124.

3.0 IMA TERMINOLOGY

Before entering the details of development and certification processes it is important to define a common set of terminology to be use with respect to integrated modular avionics.

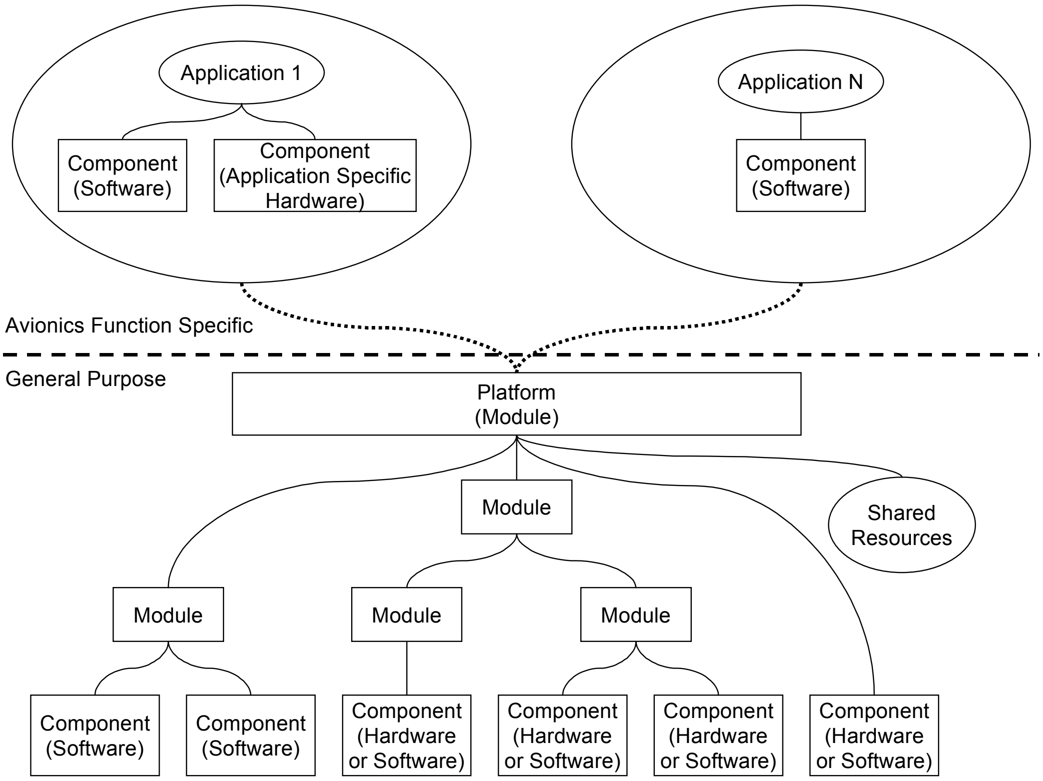

Application 1
Component (Software)
Component (Application Specific Hardware)
Application N
Component (Software)
Avionics Function Specific
General Purpose
Platform (Module)
Module
Shared Resources
Module
Module
Module
Component (Software)
Component (Software)
Component (Hardware or Software)
Component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

Figure 1: IMA terminology

The design terminology as depicted in Figure 1 [1] defines a clear distinction between IMA elements that are general purpose and those that are specific to the avionics function. When focussing on the general purpose elements there is a top-level definition for what is called a platform. In fact a platform can consist of one or more modules which can be hardware or software components. Another specific property of a platform is the fact that it has core software inside and that it can host the IMA applications.

Another important term that needs to be introduced and defined is "acceptance". Within the context of IMA this is defined as [1]: *"Acknowledgement by the certification authority that the module, application, or system complies with its defined requirements. Acceptance is recognition by the certification authority (typically in the form of a letter or stamped data sheet) signifying that the submission of data, justification, or claim of equivalence satisfies applicable guidance or requirements. The goal of acceptance is to achieve credit for future use in a certification project."* The IMA building block (i.e. platform or module), together with the certification data that has received this acceptance, can now be used in an incremental way, building up and integrating the IMA architecture. This process is called incremental acceptance. Finally, this incremental acceptance will facilitate the certification process.

4.0 INTEGRATION AND ACCEPTANCE

The development process and the certification process of IMA are very much correlated. Starting from scratch, the development process will follow a traditional V-model approach. However, ideally the development of the platform and the hosted applications is performed in parallel, which in fact forms a double-V-model. One must keep in mind that the applications can never receive stand-alone acceptance without a reference platform. Therefore, the integration steps (i.e. the upward leg of both V-models) are strongly connected, and therefore this process is better known as W-model.

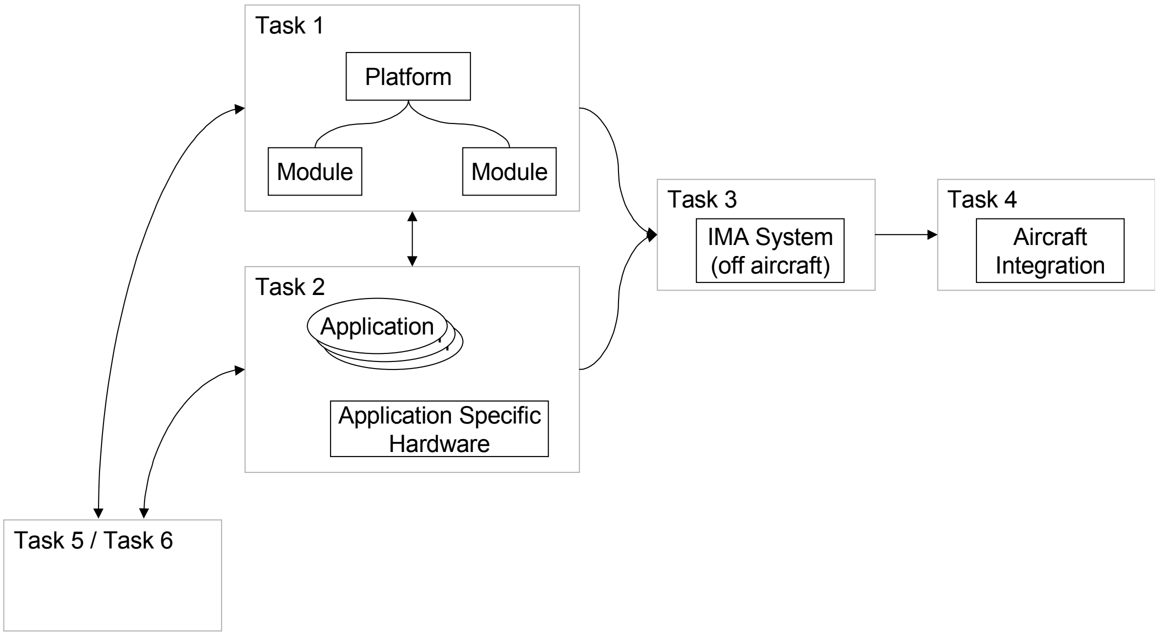


Figure 2: Certification tasks

For each integration step a certification task can be defined, as depicted in Figure 2 [1]. Starting at the lowest level (bottom of the V) the process starts with the integration of components and modules into a platform. The certification task performed here is the platform or module acceptance. Once one application gets integrated onto the platform it will result in an application acceptance. IMA acceptance is achieved when integrating multiple applications with the platform and with one another. Then the aircraft integration task is performed when integrating the IMA system within the aircraft and with the other aircraft systems. Finally, changing the IMA system or re-using the installation in another aircraft are special cases within the acceptance process.

5.0 CERTIFICATION DATA

The different certification tasks need to accepted by the certification authorities. In order to streamline this process a pre-defined set of certification data is defined. This set is strongly correlated to the know processes for defined in earlier RTCA/EUROCAE documents, for example DO-178/ED-12 [2] and DO-254/ED-80 [3].

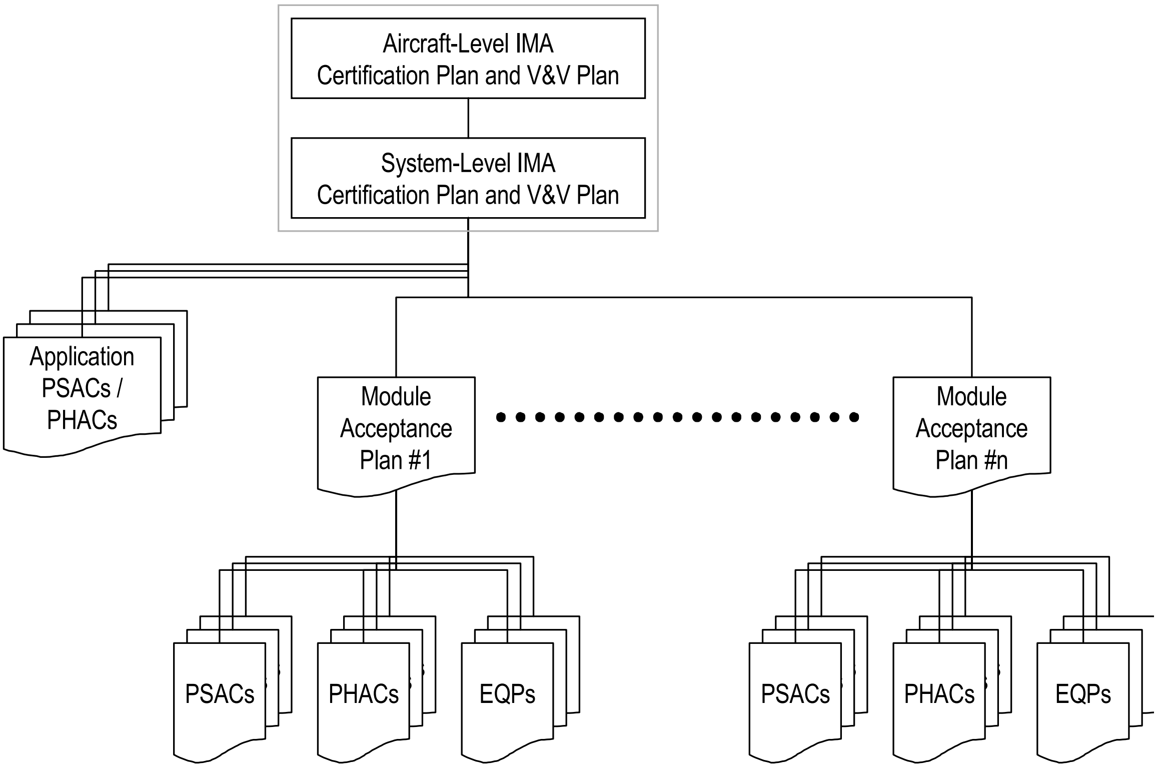


Figure 3: IMA planning data

Figure 3 [1]shows how the planning data is related within the IMA certification process. Starting at the top-level, the Aircraft-Level IMA certification plan and verification and validation (V&V) plan should describe how the process will be performed. The lower level document fit within this scheme. At the bottom level there are the traditional plans for software/hardware aspects of certification (PSAC/PHAC) together with the environmental qualification plans (EQP). The same document trees are defined for requirements data and compliance data.

6.0 CONCLUSIONS

Integrated Modular Avionics technology has introduced the possibility to fragment the certification process into several steps, which is called incremental acceptance. The incremental process will benefit from a common understanding and common approach to IMA development and certification. The document recently published by RTCA and shortly to be published by EUROCAE has a wide acceptance of both industry and certification authorities. The document provides guidance on a common development process and defines the related certification tasks. It is strongly recommended to use this guidance in future IMA projects.

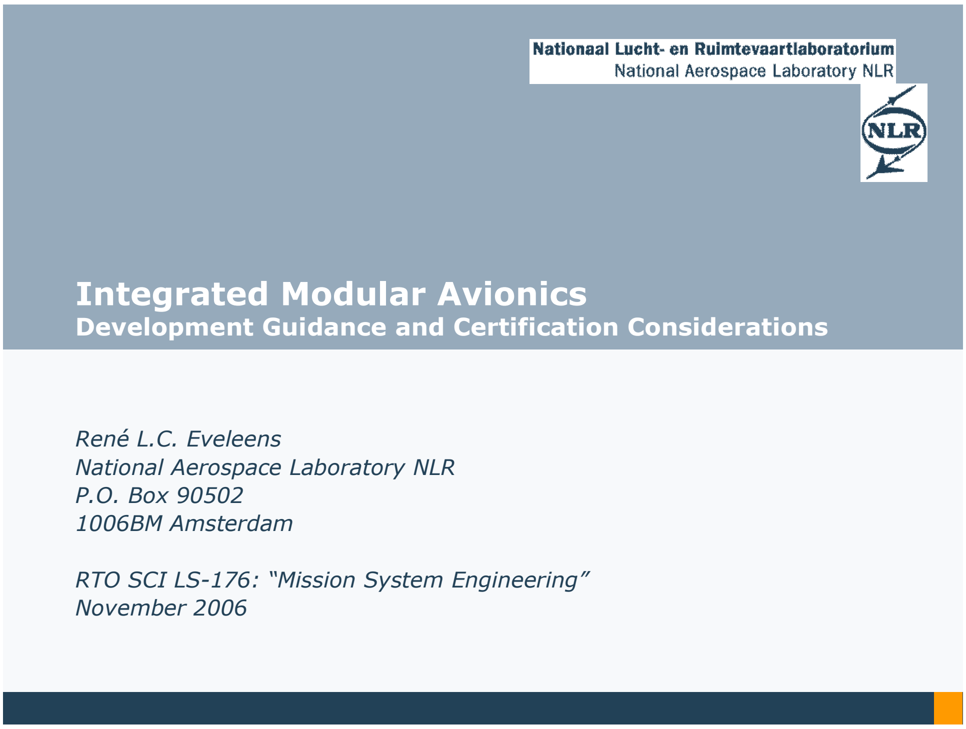
7.0 REFERENCES

[1] RTCA DO-297 / EUROCAE ED-124 (to be issued), Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

[2] RTCA DO-178 / EUROCAE ED-12, Software Considerations in Airborne Systems and Equipment Certification.

[3] RTCA DO-254 / EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware

ANNEX: PRESENTATION SLIDES



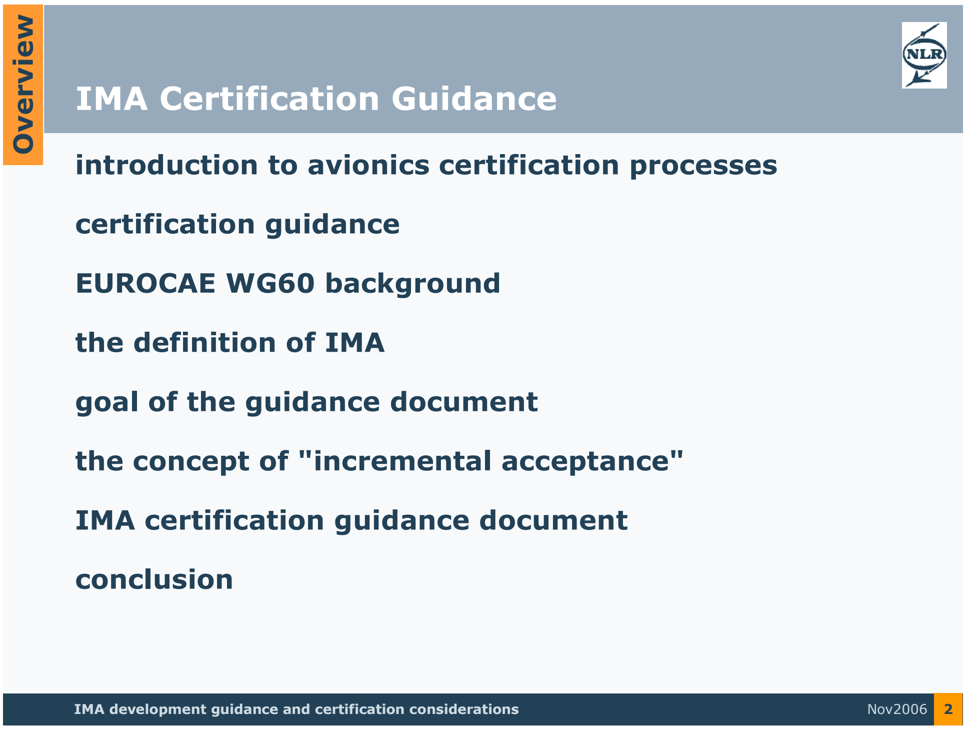
Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

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



Overview

IMA Certification Guidance

introduction to avionics certification processes

certification guidance

EUROCAE WG60 background

the definition of IMA

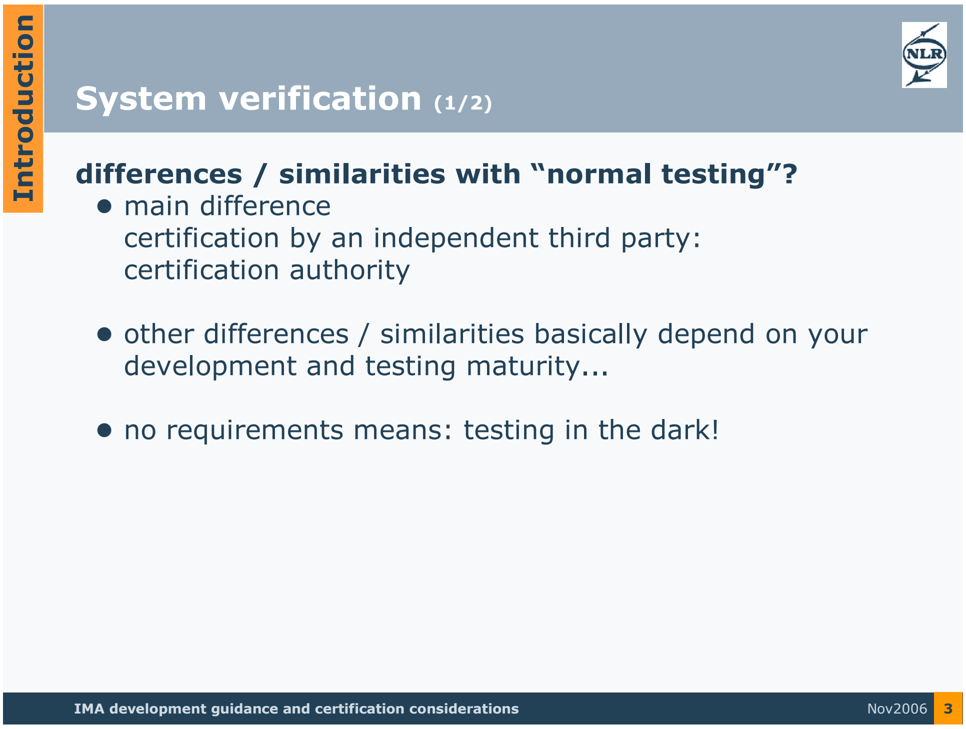
goal of the guidance document

the concept of "incremental acceptance"

IMA certification guidance document

conclusion

IMA development guidance and certification considerations Nov2006 2



Introduction

System verification (1/2)

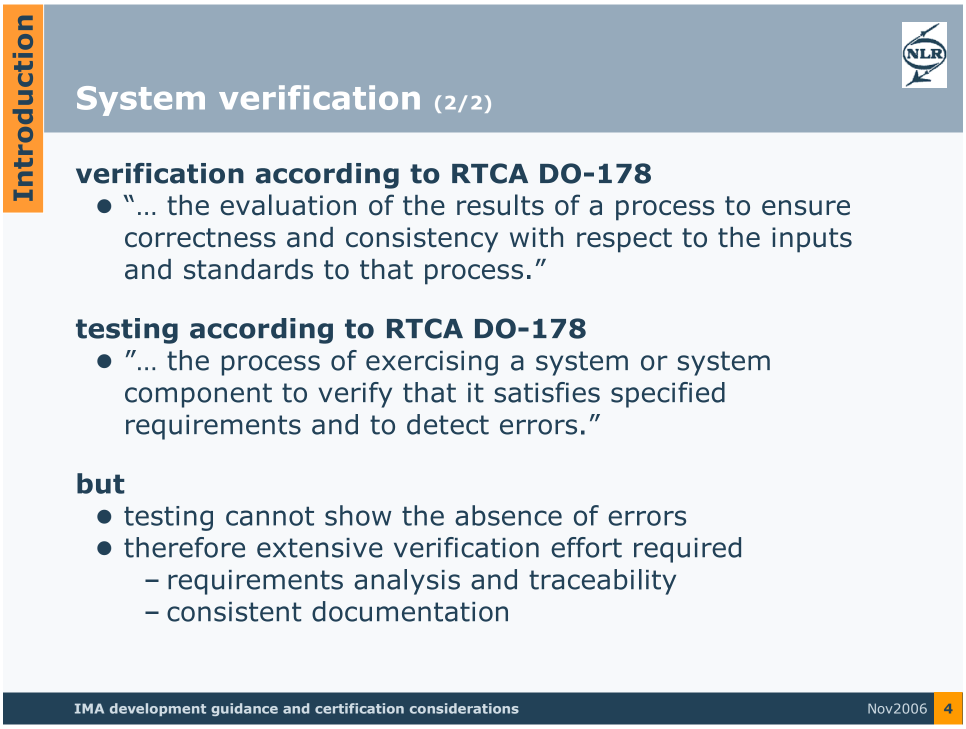
differences / similarities with "normal testing"?

- 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!

IMA development guidance and certification considerations Nov2006 3



Introduction

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."

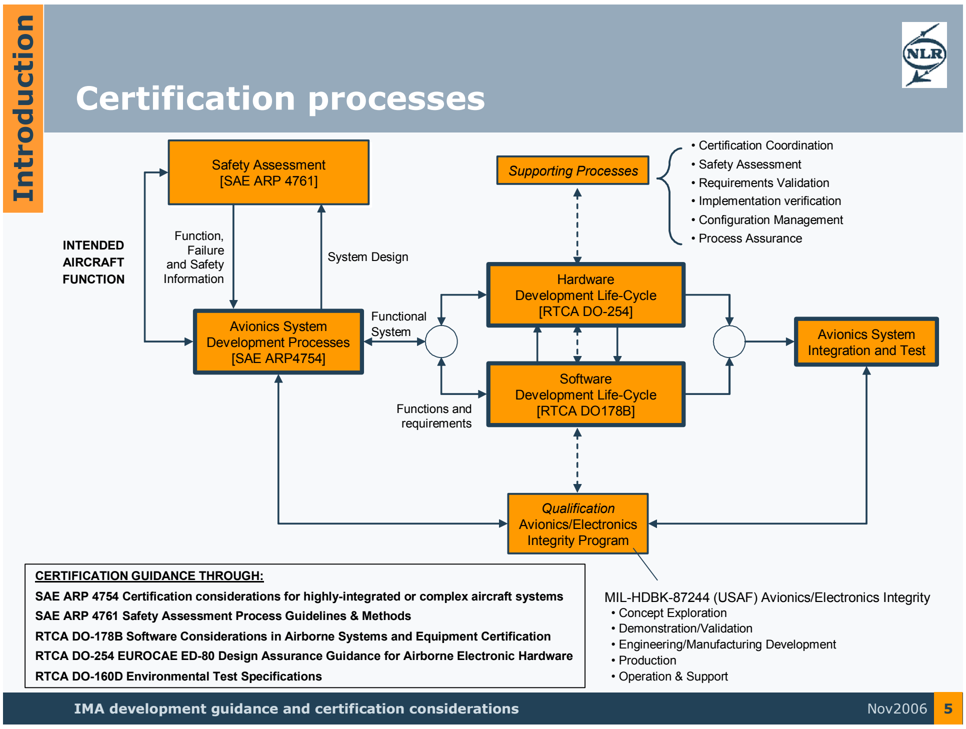
testing according to RTCA DO-178

- "… 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

IMA development guidance and certification considerations Nov2006 4



Introduction

Certification processes

Safety Assessment [SAE ARP 4761]

Supporting Processes

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

INTENDED AIRCRAFT FUNCTION

Function, Failure and Safety Information

System Design

Avionics System Development Processes [SAE ARP4754]

Functional System

Hardware Development Life-Cycle [RTCA DO-254]

Software Development Life-Cycle [RTCA DO178B]

Functions and requirements

Avionics System Integration and Test

Qualification Avionics/Electronics Integrity Program

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

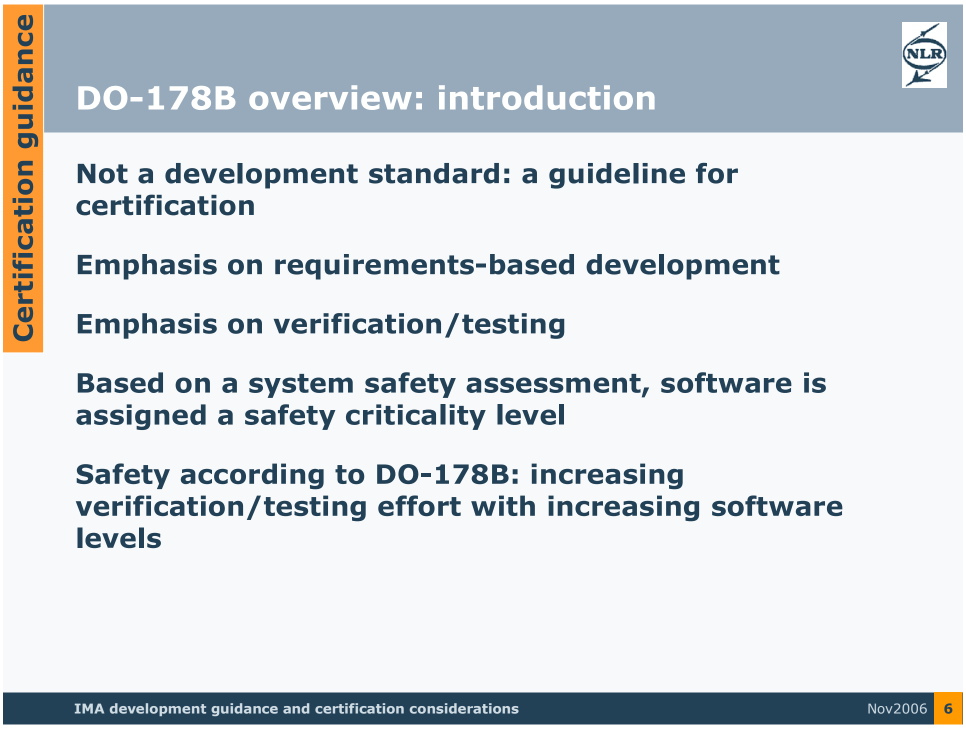
RTCA DO-254 EUROCAE ED-80 Design Assurance Guidance for Airborne Electronic Hardware

RTCA DO-160D Environmental Test Specifications

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

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

IMA development guidance and certification considerations Nov2006 5



Certification guidance

DO-178B overview: introduction

Not a development standard: a guideline for certification

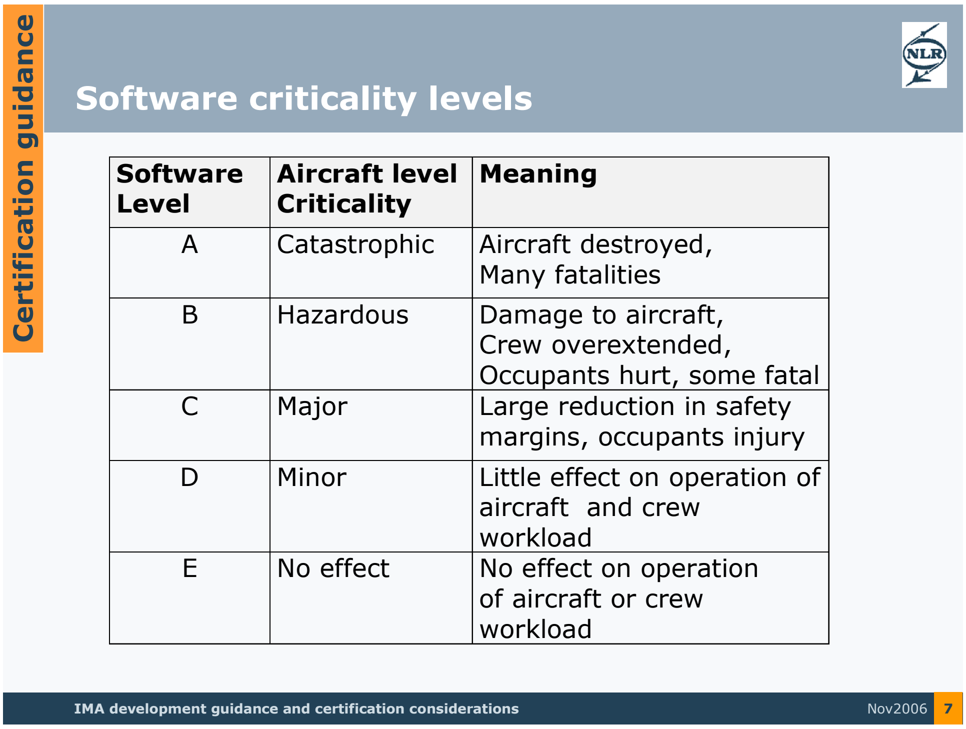
Emphasis on requirements-based development

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

IMA development guidance and certification considerations Nov2006 6

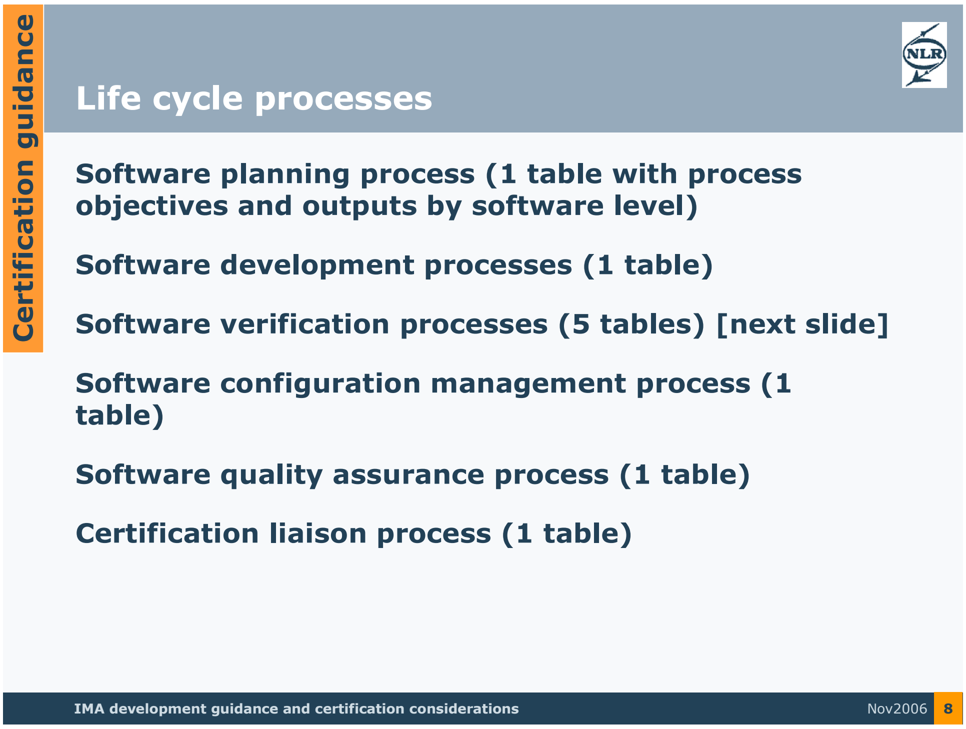


Certification guidance

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

IMA development guidance and certification considerations Nov2006 7



Certification guidance

Life cycle processes

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

Software development processes (1 table)

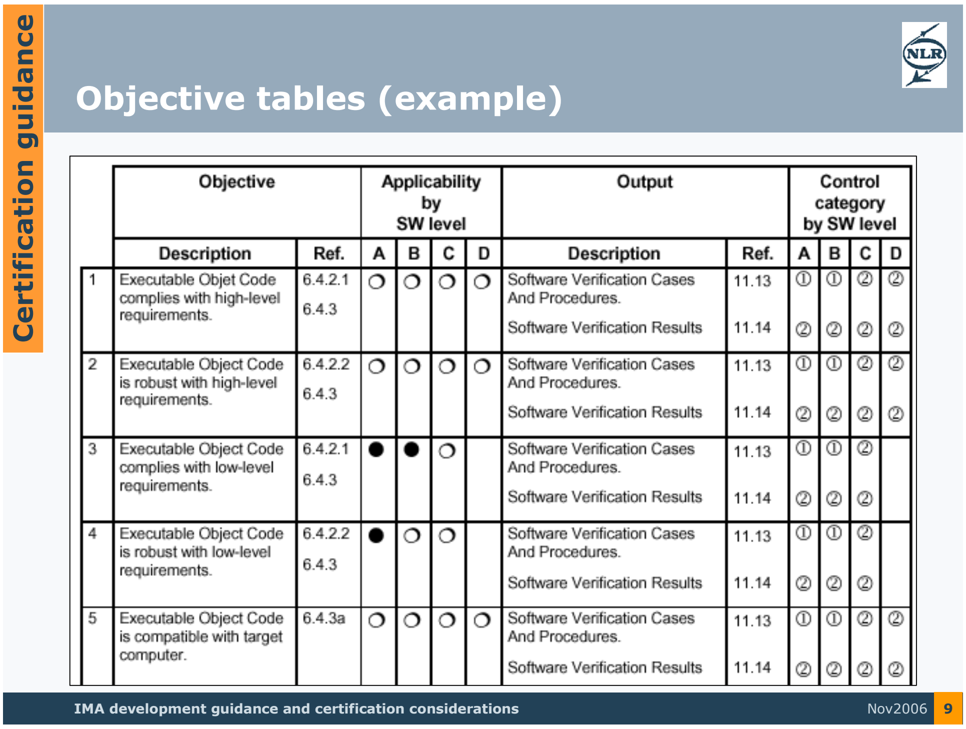
Software verification processes (5 tables) [next slide]

Software configuration management process (1 table)

Software quality assurance process (1 table)

Certification liaison process (1 table)

IMA development guidance and certification considerations Nov2006 8

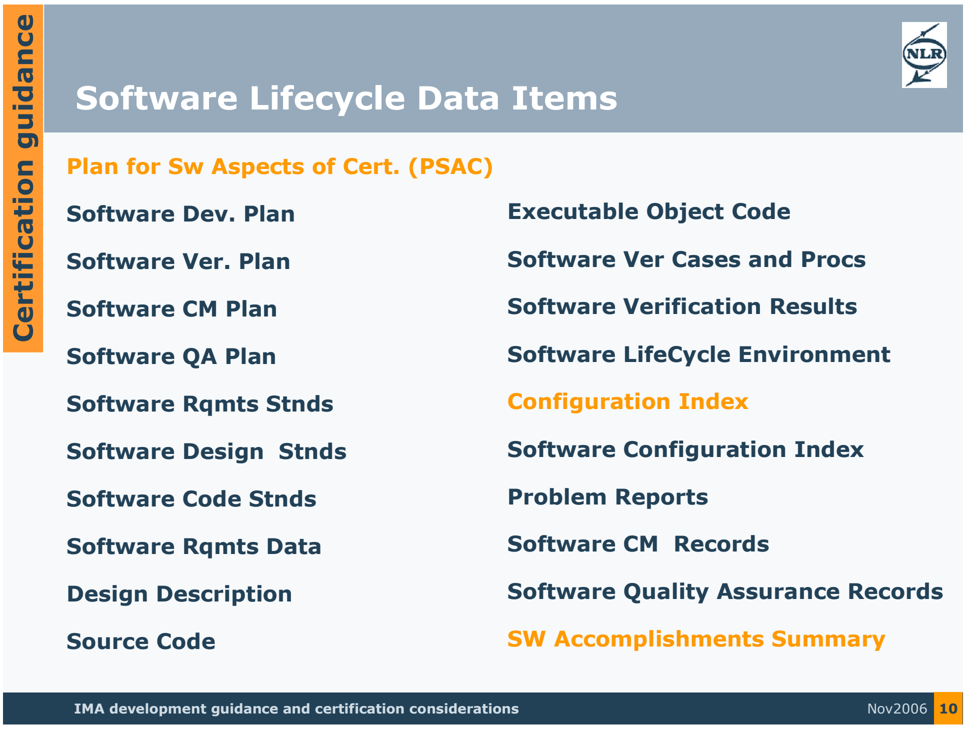


Certification guidance

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

IMA development guidance and certification considerations Nov2006 9



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

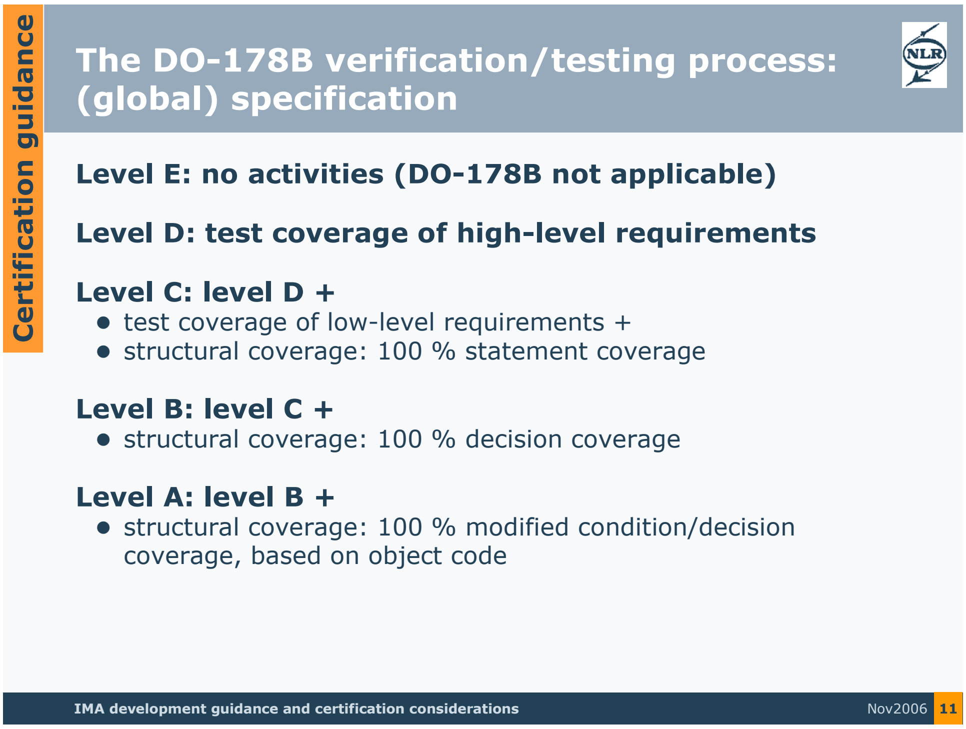
Problem Reports

Software CM Records

Software Quality Assurance Records

SW Accomplishments Summary

IMA development guidance and certification considerations Nov2006 10



Certification guidance

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

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

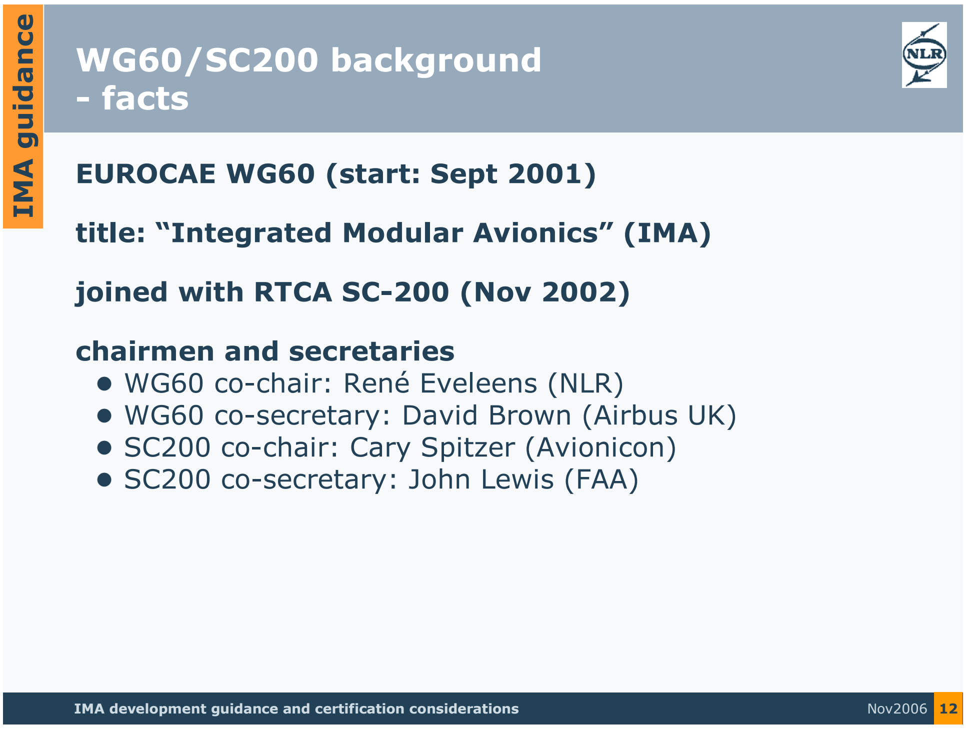
Level D: test coverage of high-level requirements

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

IMA development guidance and certification considerations Nov2006 11



IMA guidance

WG60/SC200 background - facts

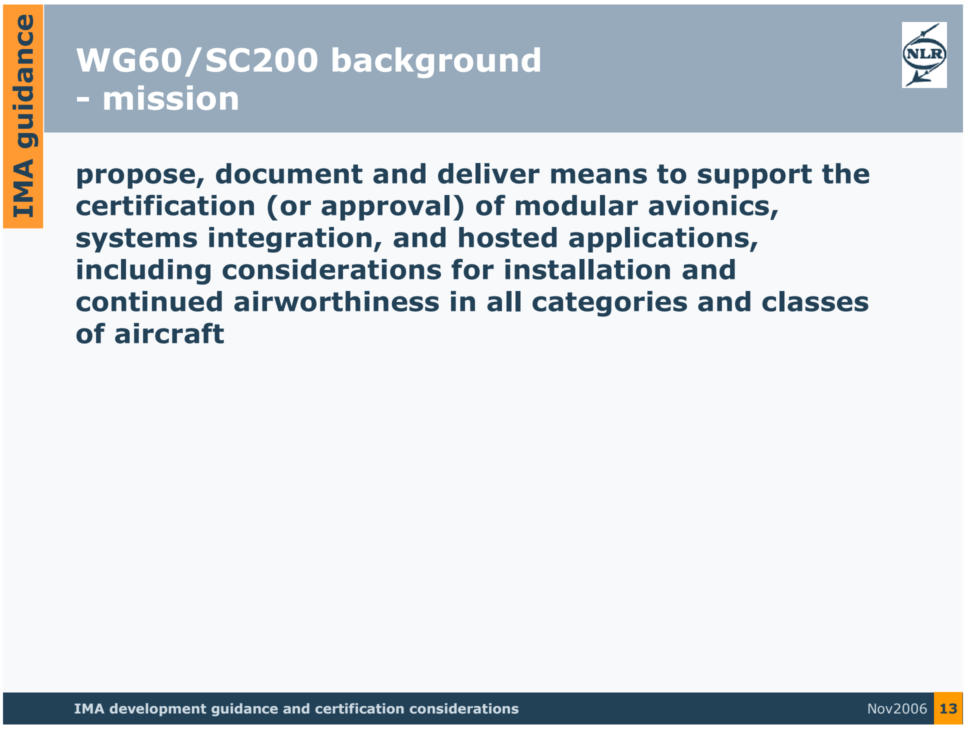
EUROCAE WG60 (start: Sept 2001)

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)

IMA development guidance and certification considerations Nov2006 12

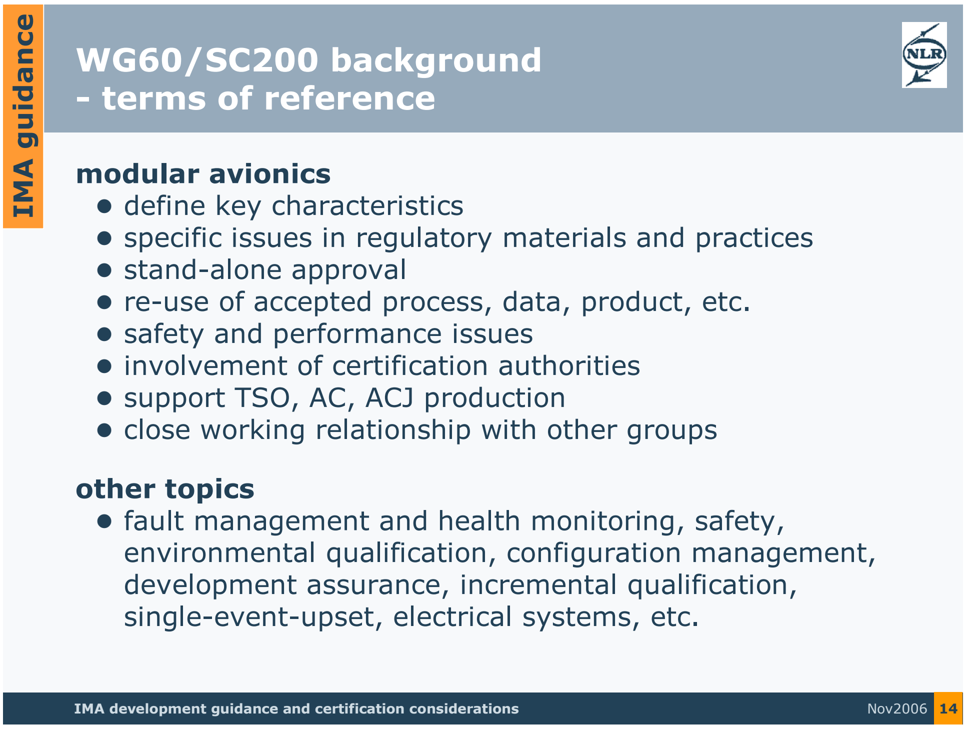


IMA guidance

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

IMA development guidance and certification considerations Nov2006 13



IMA guidance

WG60/SC200 background - terms of reference

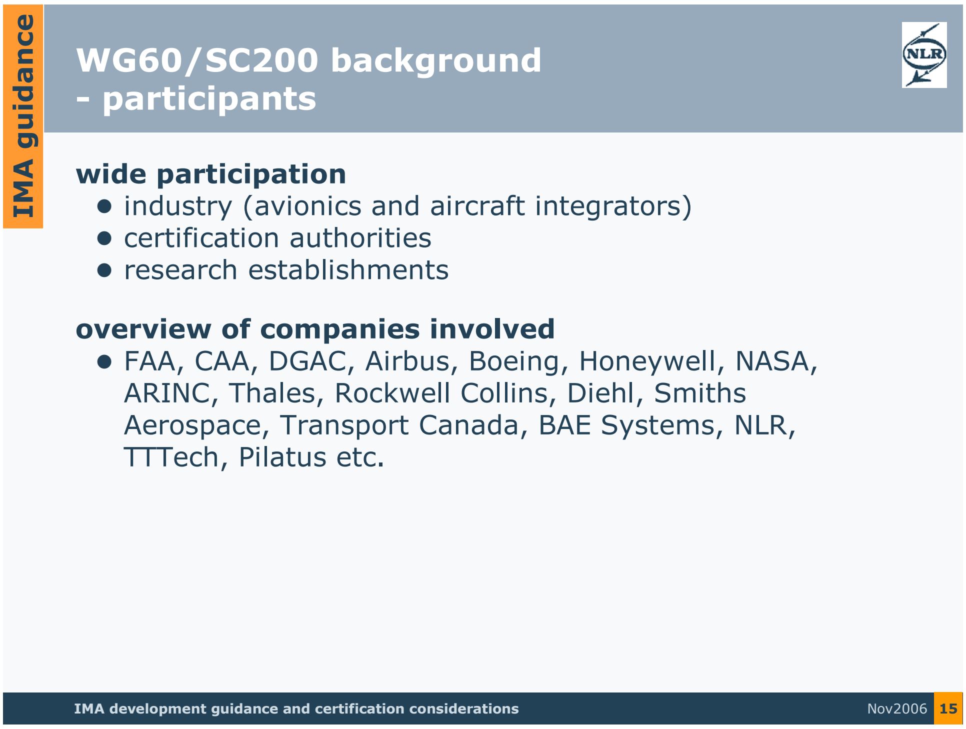
modular avionics

- 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.

IMA development guidance and certification considerations Nov2006 14



IMA guidance

WG60/SC200 background - participants

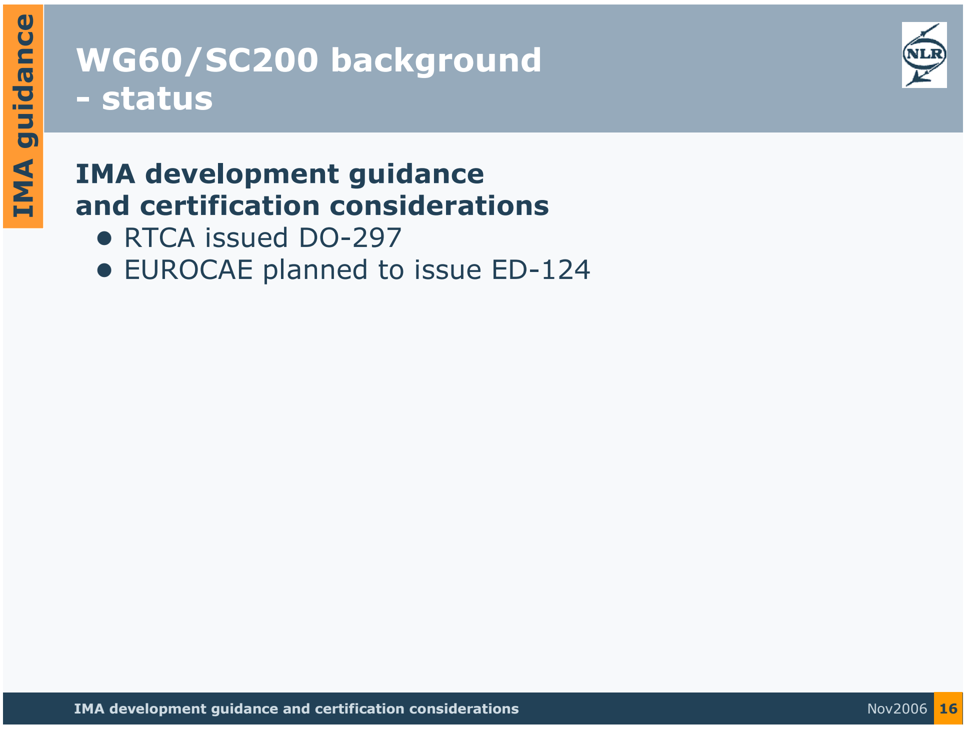
wide participation

- 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.

IMA development guidance and certification considerations Nov2006 15



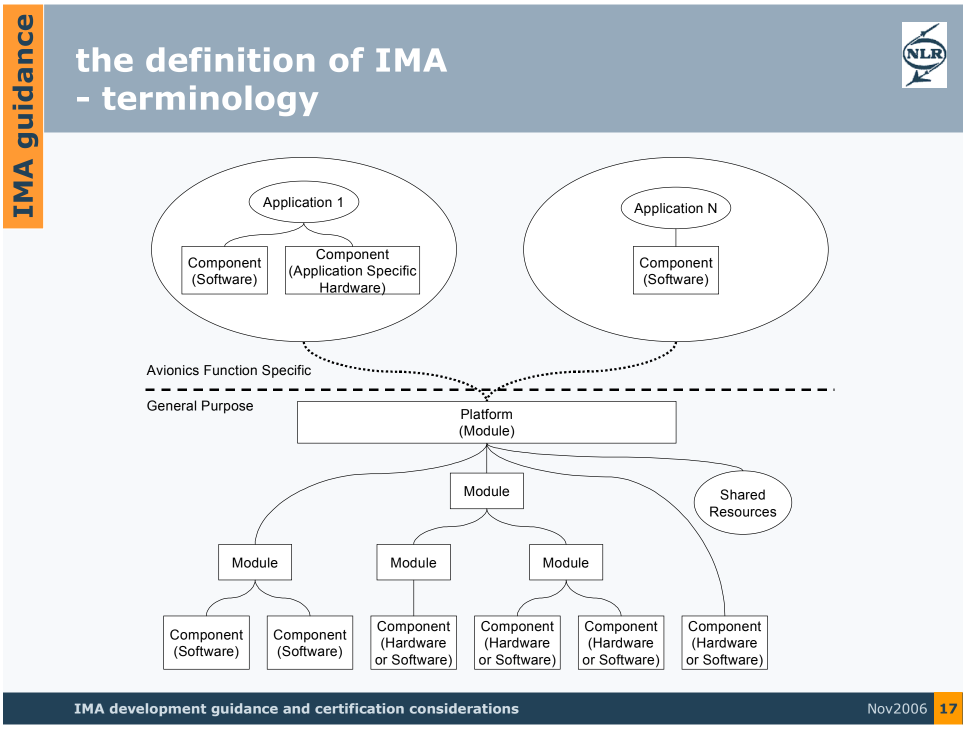
IMA guidance

WG60/SC200 background - status

IMA development guidance and certification considerations

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

IMA development guidance and certification considerations Nov2006 16

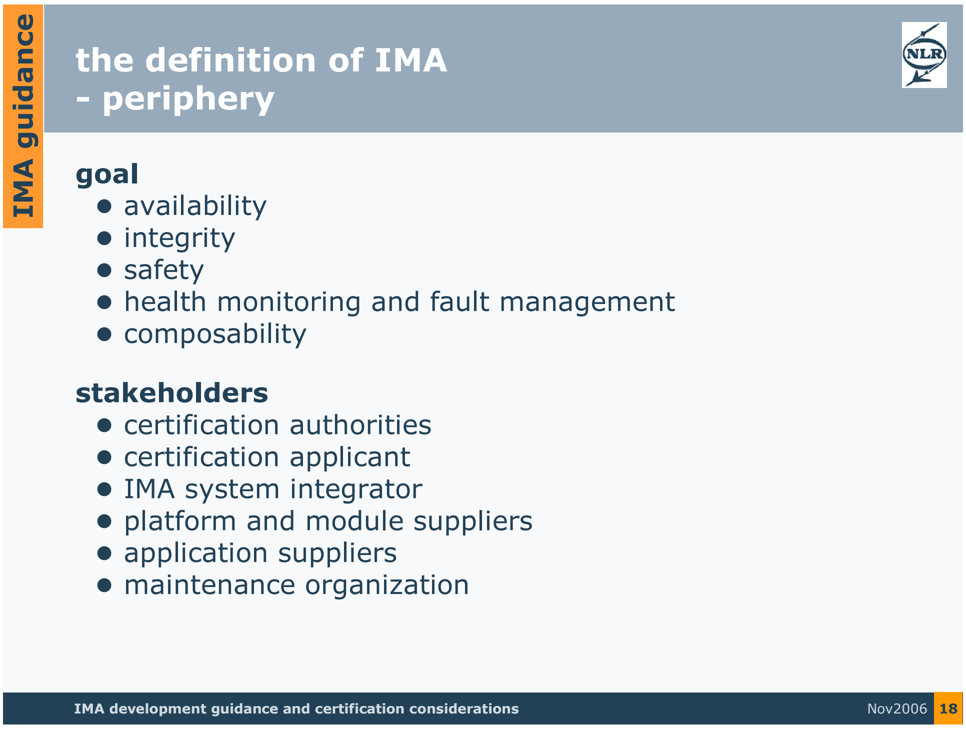


IMA guidance

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)

IMA development guidance and certification considerations Nov2006 17



IMA guidance

the definition of IMA - periphery

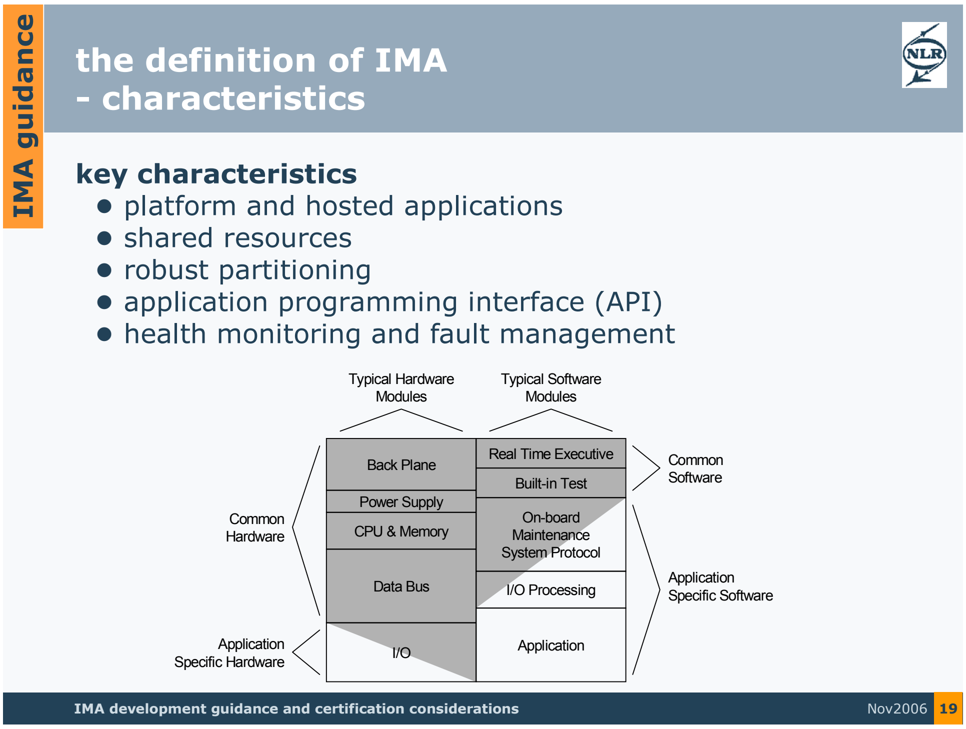
goal

- 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

IMA development guidance and certification considerations Nov2006 18



IMA guidance

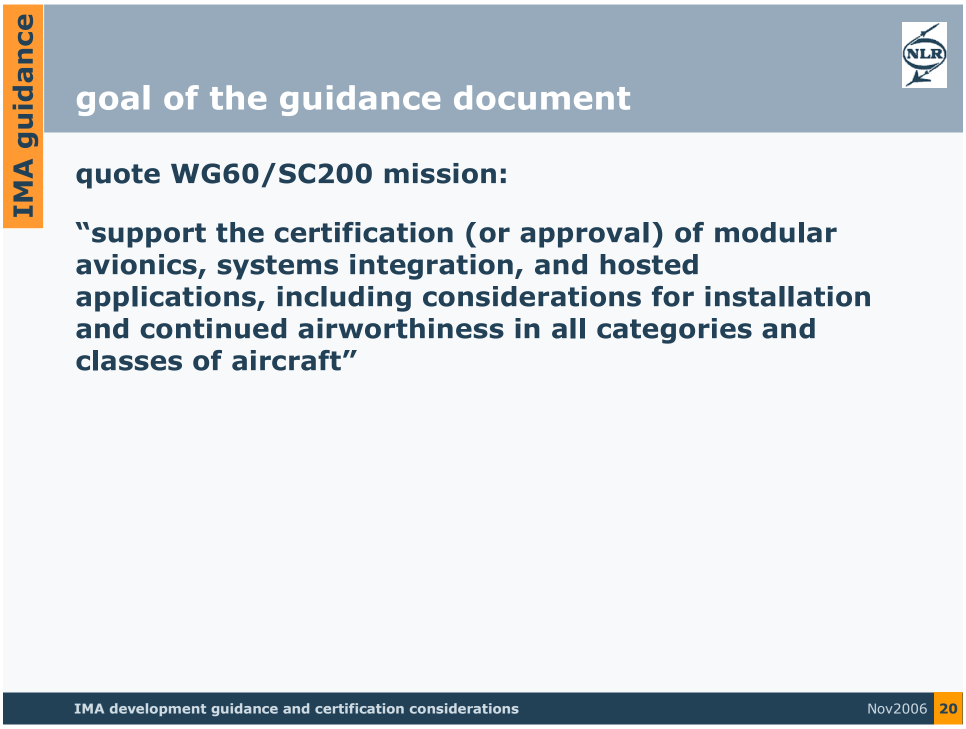
the definition of IMA - characteristics

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

IMA development guidance and certification considerations Nov2006 19



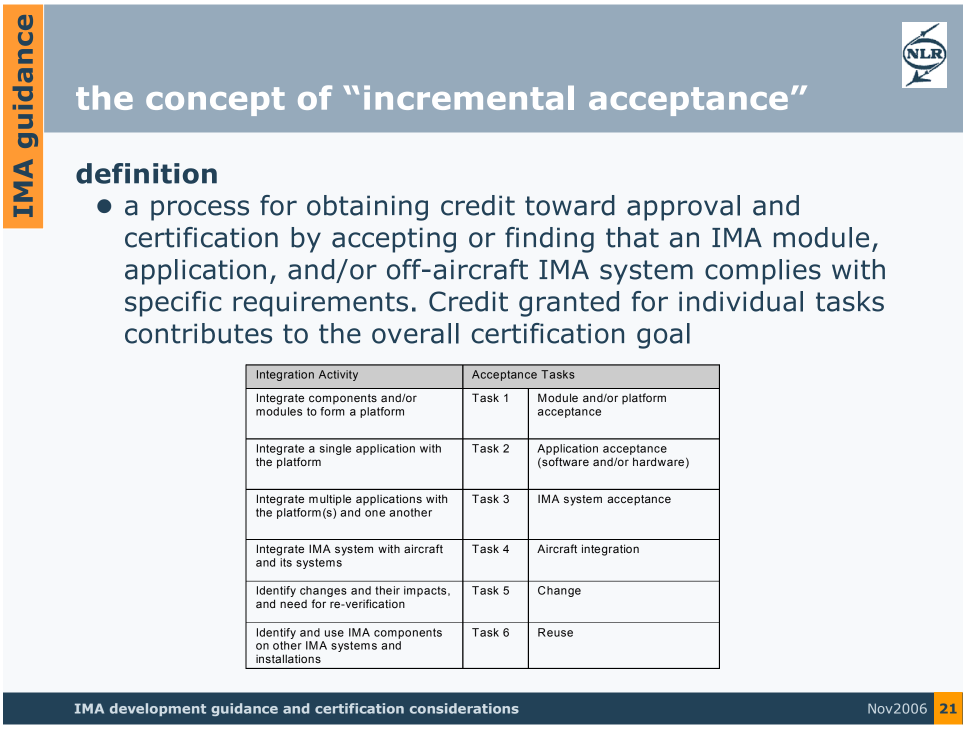
IMA guidance

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"

IMA development guidance and certification considerations Nov2006 20



IMA guidance

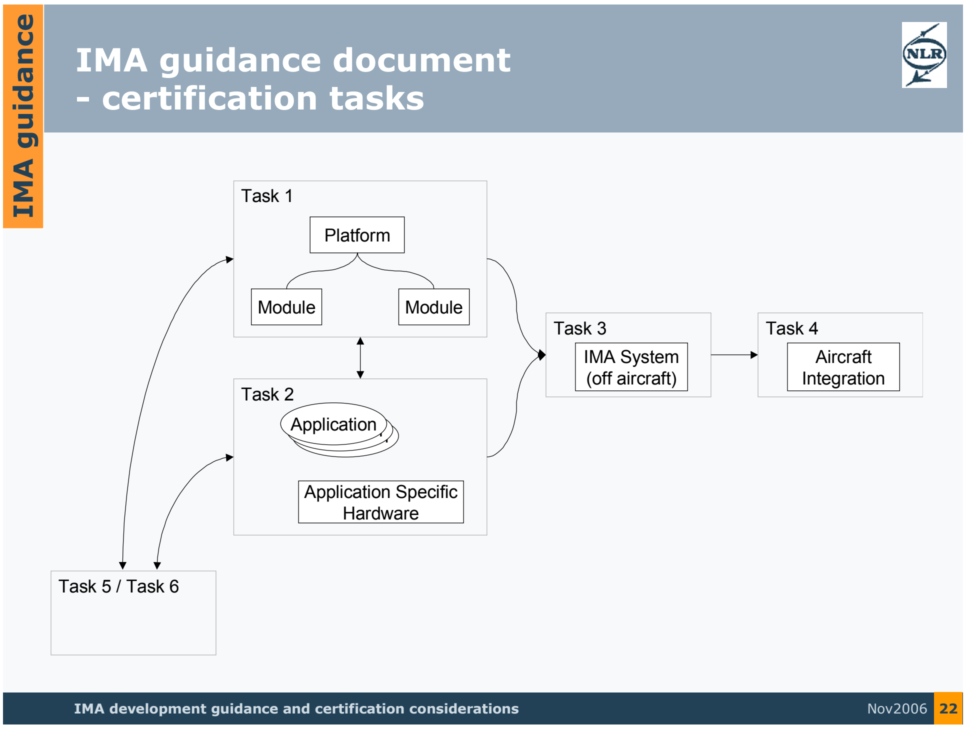
the concept of "incremental acceptance"

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

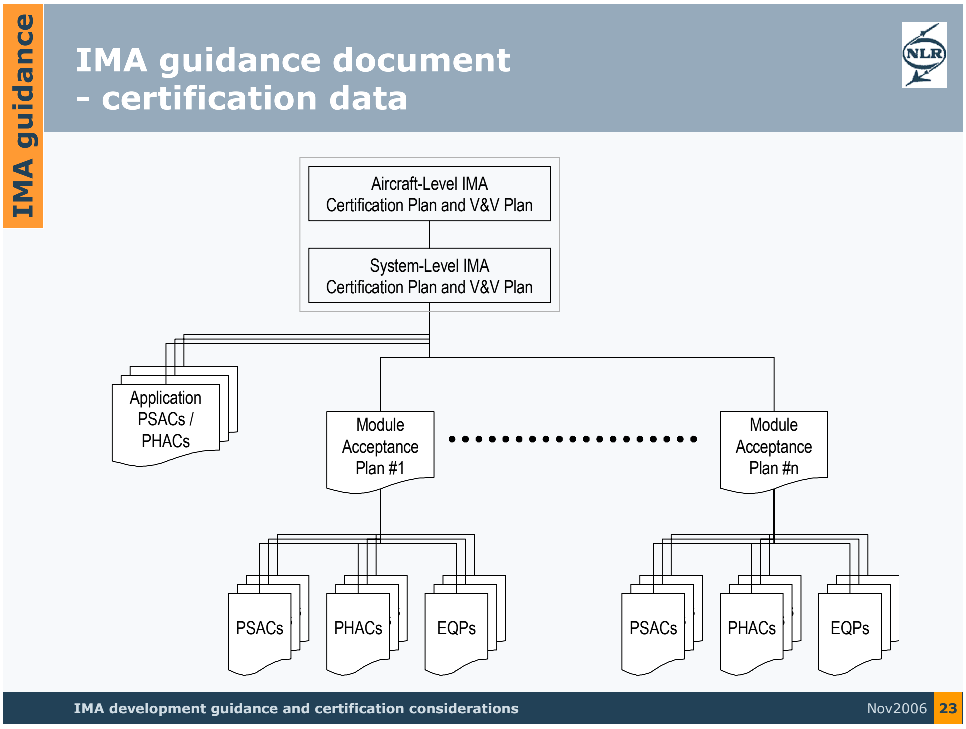
IMA development guidance and certification considerations Nov2006 21



IMA guidance

IMA guidance document - certification tasks

IMA development guidance and certification considerations Nov2006 22



IMA guidance

IMA guidance document - certification data

Aircraft-Level IMA Certification Plan and V&V Plan

System-Level IMA Certification Plan and V&V Plan

Application PSACs / PHACs

Module Acceptance Plan #1

Module Acceptance Plan #n

PSACs

PHACs

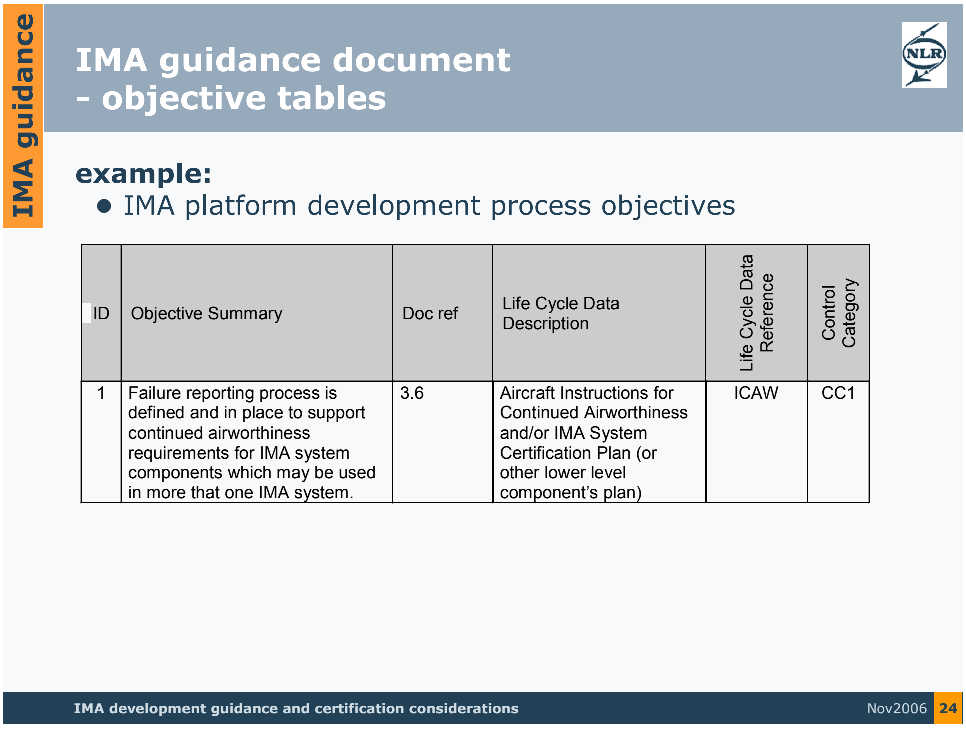
EQPs

PSACs

PHACs

EQPs

IMA development guidance and certification considerations Nov2006 23



IMA guidance

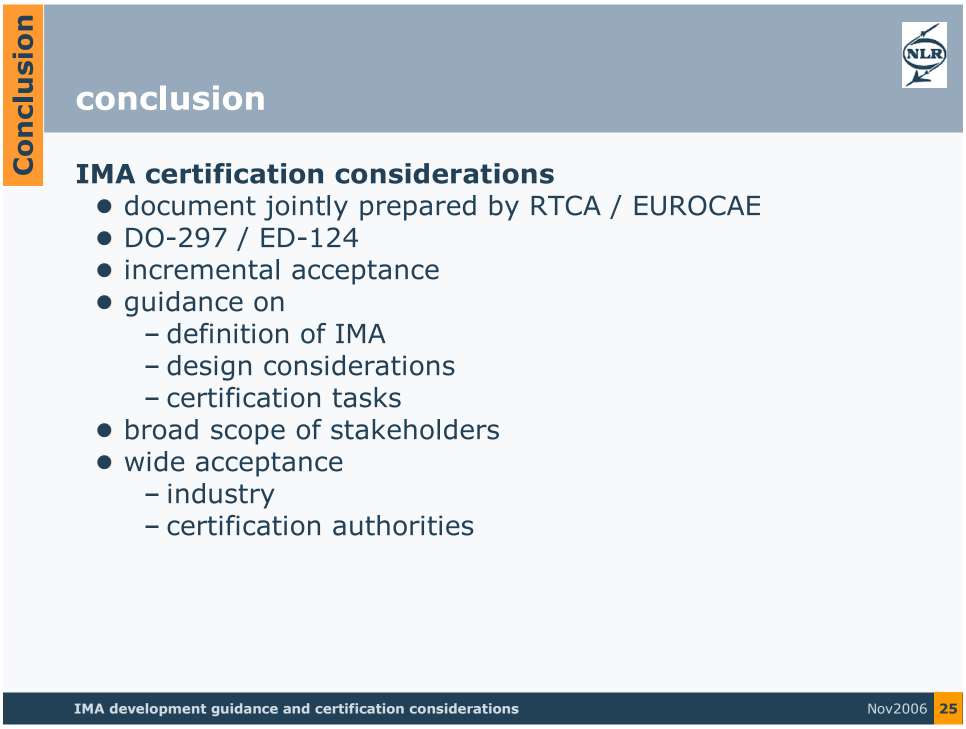
IMA guidance document - objective tables

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

IMA development guidance and certification considerations Nov2006 24



Conclusion

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

IMA development guidance and certification considerations Nov2006 25