

# DO-178C/ED-12C

## Impact, bilan et perspectives

***Action collective « Certification avionique »  
Une démarche d'accompagnement proposée par JESSICA France avec le  
soutien financier de DIRRECTE et de la Région Midi-Pyrénées***

**Présentée par Frederic POTHON**  
[frederic.pothon@acg-solutions.fr](mailto:frederic.pothon@acg-solutions.fr)  
[www.acg-solutions.fr](http://www.acg-solutions.fr)



**Avec le concours de Gérard LADIER**  
**Airbus/Aerospace Valley**  
**Chairman du WG71**

**18 Septembre 2013**  
**LAAS/CNRS - TOULOUSE**

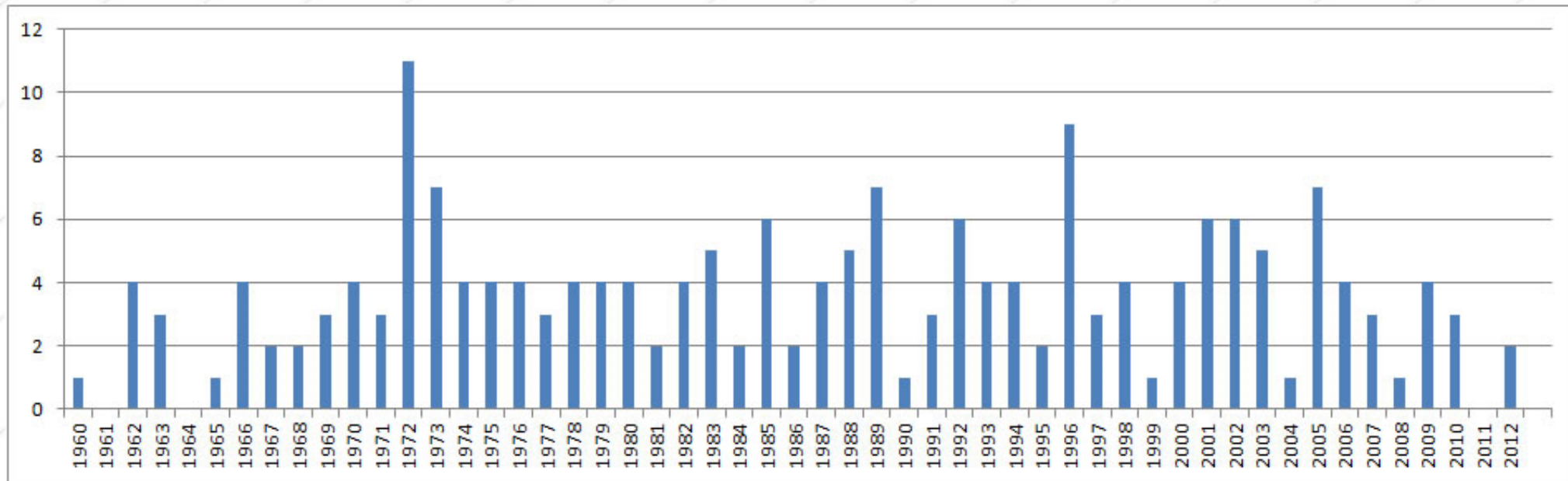
# DO-178C/ED-12C

## Impact, bilan et perspectives

1. Why?
2. Application
3. Impact
4. Additional documents
5. FAS for the future

# 1- A new release: Why?

**Number Of Accidents With 100 Or More Fatalities By Year**



# 1- Context

## 1.1 Introduction

For equipments and systems: FAR/CS  
25.1309 (large aeroplanes)

### Airworthiness Regulation Requirements

Federal Airworthiness Requirements / Joint Airworthiness Requirements (EASA)



FAR - CS 25.1309 « Equipment, Systems and Installations »

AC - AMC 25.1309 « System design and analysis »

Equipment

**1 serious accident each  $10^6$  flight hours**

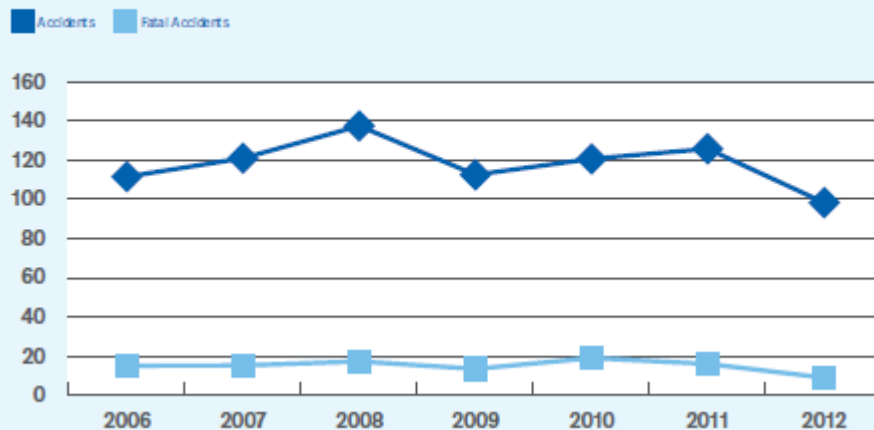
# 1- A new release: Why?

## Some statistics (Source: IATA 2013)

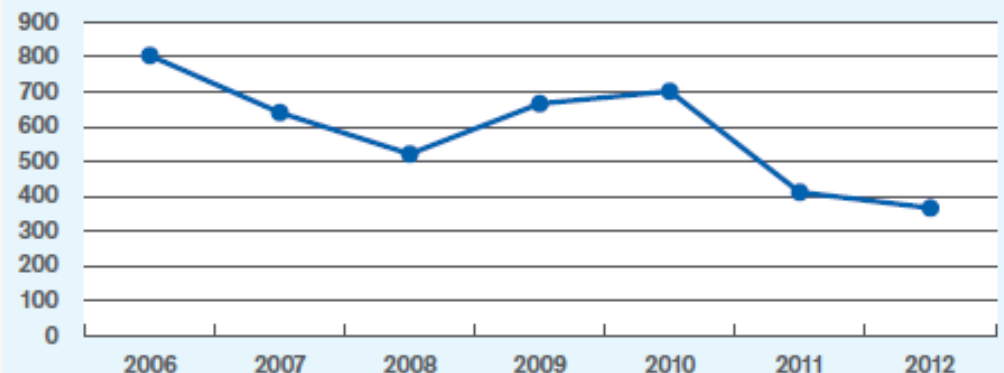
**2.4 accidents per million departures**

This combined rate represents a 33 per cent improvement in industry performance over 2011. ICAO and IATA will continue their efforts through the GSIE to align analysis methodologies in order to achieve greater harmonization in accident reporting with all involved industry stakeholders.

Accident Trends: 2006–2012



Fatality Trends: 2006–2012



# 1- A new release: Why?

08/25/2010	Filair	Bandundu, Congo Democratic Republic	A passenger brought aboard a crocodile hidden in a sports bag. The crocodile escaped, causing a panic among passengers who all rushed to one end of the plane. This caused an imbalance in the aircraft which led to loss of control and a crash.
------------	--------	-------------------------------------	---

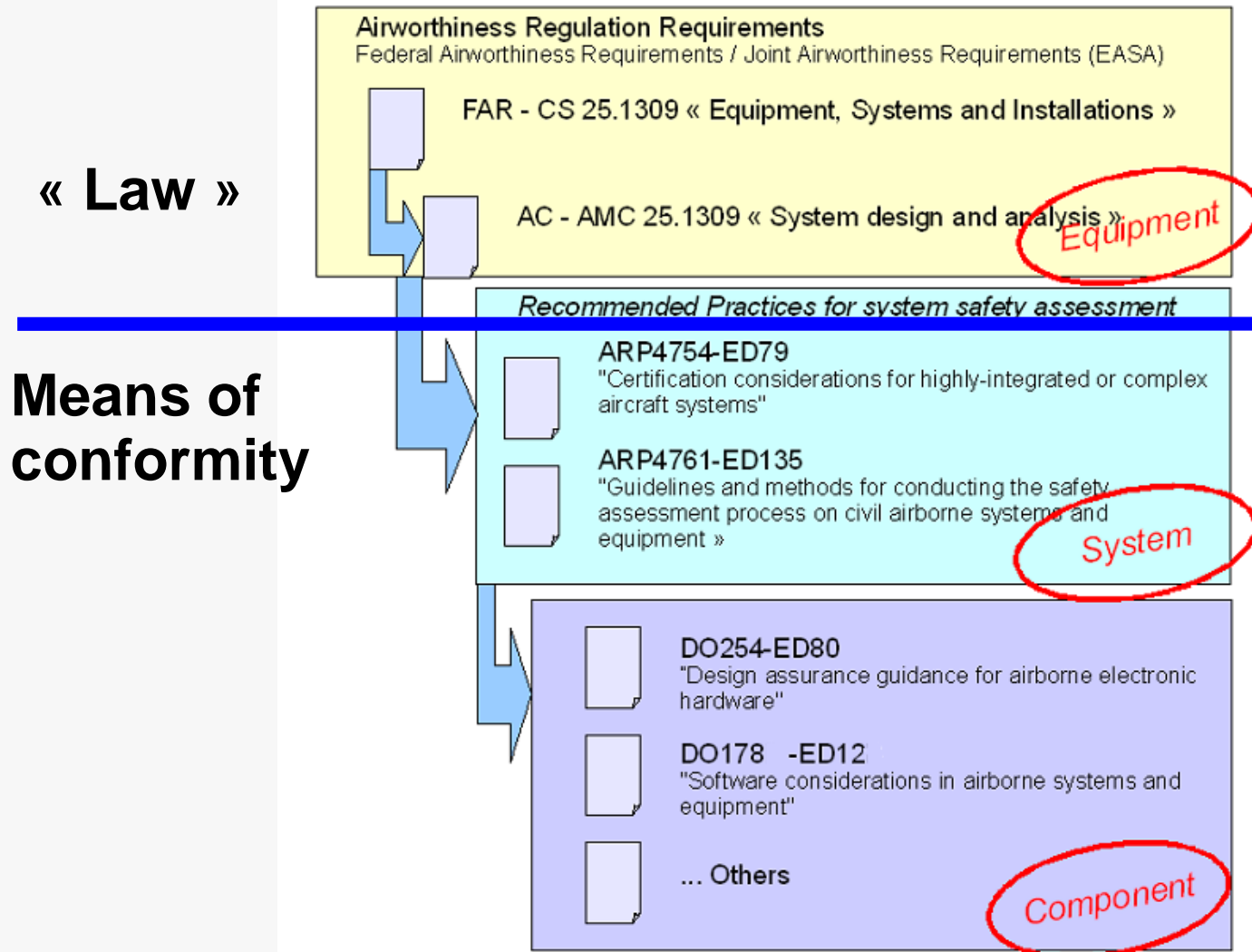
# 1- A new release: Why?

## Some statistics (Source: IATA 2013)

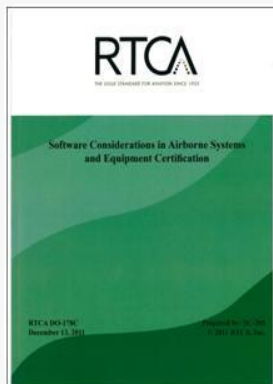
### Accident Categories

Code	Description	Accidents	With fatalities	Fatalities
CFIT	Controlled flight into/towards terrain	3	1	127
RS	Runway safety-related	43	2	11
LOC-I	Loss of control in-flight	2	1	31
F-NI	Fire – non-impact	2	0	0
TURB	Turbulence encounter	18	0	0
OTH	Other	8	0	0
UNK	Unknown	9	4	184
SCF	System component failure	14	1	19
		99	9	372

# 1- A new release: Why?



DO-178/ED-12 provides acceptable means for assessing and controlling the software used to program digital-computer-based systems





# 1- A new release: Why?

**Does DO-178B/ED-12B not rigorous enough? Is there any gaps?**

**NO**

More than 15 years of DO-178B/ED-12B usage, has not revealed any major safety flaws.

# 1- A new release: Why?

**Is it difficult to apply DO-178B/ED-12B to new methods and technologies?**

**YES**

New software methods, tools, techniques emerged in software area.

But,

- Safety constraints => Fears on novelties
- Not explicitly addressed => Difficult to apply
- No background => Approval risks

***Difficult to use more efficient and more safe methods!***

# 1- A new release: Why?


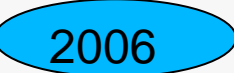







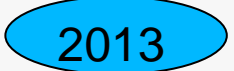
**Is the text stable, and widely applied with a common interpretation?**

**NO**

The text didn't change, but could be an illusion as

- The way to understand is evolving
- Additional information exists (DO-248/ED-94)
- CAST papers, Clarification paper, CRIs are accumulating, not always consistent, and are not the result of a consensus

## 2- DO-178C/ED-12C application

- Step 1: RTCA/EUROCAE Joint Committee launch with approved TOR (Term of reference)  
- Step 2: Text approved by working group  
- Step 3: EUROCAE/RTCA public consultation
- Step 4: EUROCAE/RTCA approval and publication  
- Step 5: Public consultation by Certification Authorities
- Step 6: Accepted as mean of compliance by FAA/EASA (and others)
- FAA: AC 20-115C: published.  
- EASA: AMC 20-115C: Expected end of year  
- Step 7: Application on new programs

2014

# 3- A new release: Impact

Five types of changes in the core text

- Errors
- Consistent terminology
- Clarifications
- Hidden objectives
- New topics

# 3- A new release: Impact

## Errors:

Most of them already identified in DO-248B/ED-94B

- Typo
- Wrong references
- Compiler aspects: Now identified in integration process
- Control category for some development data for level C

**No impact**

# 3- A new release: Impact

## Consistent terminology

- Text clean up: guidance/guideline
- Consistency between objective table and text
- Better identification of activities

**No impact**

# 3- A new release: Impact

**Consistent terminology** : SCM Objectives not defined!

**Activities are referenced here!**

Table A-8 Software Configuration Management Process

	Objective		Applicability by SW Level				Output		Control Category by SW level					
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D		
1	Configuration items are identified.	7.2.1	○	○	○	○	SCM Records	11.18	○	○	○	○		
2	Baselines and traceability are established.	7.2.2	○	○	○	○	Software Configuration Index	11.16	⊕	⊕	⊕	⊕		
			SCM Records	11.18	○	○	○	○						
3	Problem reporting, change control, change review, and configuration status accounting are established.	7.2.3 7.2.4 7.2.5 7.2.6	○	○	○	○	Problem Reports	11.17	○	○	○	○		
			SCM Records	11.18	○	○	○	○						
			Archive, retrieval, and release are established.	7.2.7	○	○	○	○	SCM Records	11.18	○	○	○	○
			Software load control is established.	7.2.8	○	○	○	○	SCM Records	11.18	○	○	○	○
6	Software life cycle environment control is established.	7.2.9	○	○	○	○	Software Life Cycle Environment Configuration Index	11.15	⊕	⊕	⊕	○		
			SCM Records	11.18	○	○	○	○						



# 3- A new release: Impact

**Consistent terminology** : Activities identification in the tables

**TABLE A-6  
TESTING OF OUTPUTS OF INTEGRATION PROCESS**

	Objective		Activity	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref		Ref	A	B	C	D	Data Item	Ref	A	B	C
3	Executable Object Code complies with low-level requirements.	6.4.c	6.4.2 6.4.2.1 6.4.3 6.5	●	●	○		Software Verification Cases and Procedures	11.13	①	①	②	
								Software Verification Results	11.14	②	②	②	
								Trace Data	11.21	①	①	②	

“Recommended” Activities

*6.4.2 Requirements-Based Test Selection*

*6.4.2.1 Normal Range test Cases*

*6.4.3 Requirement-Based testing Methods*

*6.5 Software Verification Process Traceability*

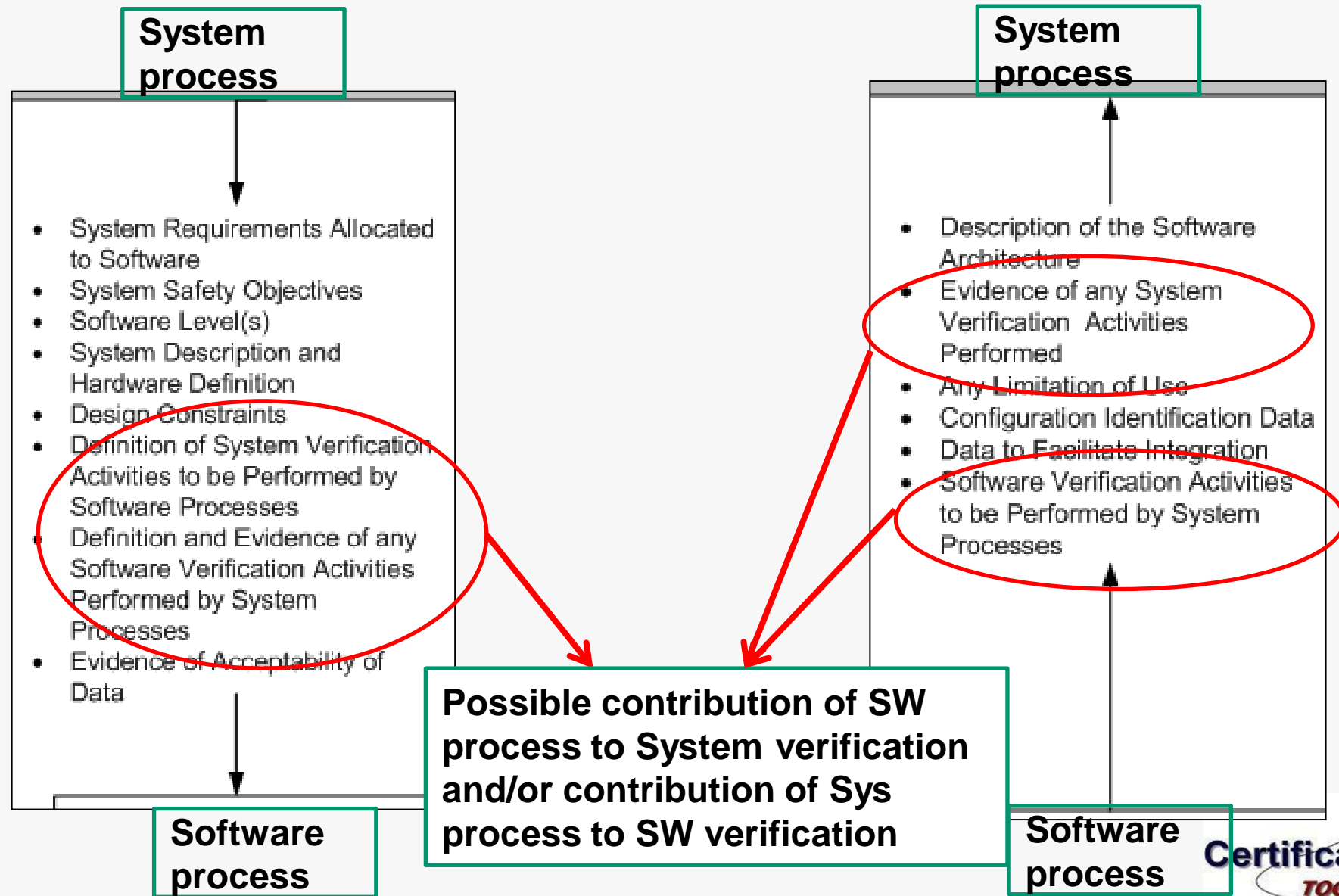
# 3- A new release: Impact

- Errors:
- Consistent terminology
- Clarifications:
  - Consistency with ARP4754
  - Several sections reworked for better understanding

**Normally, no impact, if correct understanding of DO-178B/ED-12B!**

# 3- A new release: Impact

## Clarifications : Sys/Sw processes



# 3- A new release: Impact

## Clarifications : Trace data and traceability

A new software life cycle data

Trace data – Data providing evidence of traceability of development and verification processes' software life cycle data without implying the production of any particular artifact. Trace data may show linkages, for example, through the use of naming conventions or through the use of references or pointers either embedded in or external to the software life cycle data.

Which *purpose* is to:

- Enable verification of the complete implementation of higher level of requirements
- Give visibility to those requirements that are not directly traceable to higher level of requirements

# 3- A new release: Impact

## Clarifications : Derived requirements (More controversial!)

### New definition

Derived requirements – Requirements produced by the software development processes which (a) are not directly traceable to higher level requirements, and/or (b) specify behavior beyond that specified by the system requirements or the higher level software requirements.

- So a derived requirement may now be traceable or partially traceable to the higher level of requirements
- Inconsistent with the purpose of the trace data “To give visibility to the requirements that are not directly traceable to the higher level of requirements”
- What is the benefit to provide “derived requirements” which do not specify behaviour beyond that specified by system requirements?

# 3- A new release: Impact

## Clarifications : Robustness

... is requirement based tests!

Failure modes, incorrect inputs ..; are defined ion the requirements and test cases are developed based on these requirements!

Note: Robustness test cases are requirements-based. The robustness testing criteria cannot be fully satisfied if the software requirements do not specify the correct software response to abnormal conditions and inputs.

# 3- A new release: Impact

## Clarifications : Data and control coupling

Part of the structural coverage analysis

- Purpose : § 6.4.4.2

This analysis determines which code structure, including interfaces between components, was not exercised by the requirements-based test procedures.

- Objective § 6.4.4.d

d. Test coverage of software structure, both data coupling and control coupling, is achieved.

- Activity § 6.4.4.2.c: Analysis based on requirements-based test!

c. Analysis to confirm that the requirements-based testing has exercised the data and control coupling between code components.

# 3- A new release: Impact

## Clarifications : Deactivated code

- Identification during planning process
- “Designing for deactivated code”, emphasis need for deactivation mechanisms
- Verification coverage, with 2 categories

d. Deactivated code: **Deactivated code should be handled in one of two ways, depending upon its defined category:**

1. **Category One**: Deactivated code that is not intended to be executed in any current configuration used within ~~an aircraft or engine~~ **any certified product**. **For this category**, a combination of analysis and testing should show that the means by which ~~such~~ **the deactivated** code could be inadvertently executed are prevented, isolated, or eliminated.
2. **Category Two**: Deactivated code that is only executed in certain approved configurations of the target computer environment. The operational configuration needed for normal execution of this code should be established and additional test cases and test procedures developed to satisfy the required coverage objectives.



# 3- A new release: Impact

- Errors:
- Consistent terminology
- Clarifications
- Hidden Objectives
  - “Implicit objectives”, not identified in the tables

**Normally, no impact, if correct understanding of DO-178B/ED-12B!**

# 3- A new release: Impact

## Objectives: Development processed for level D

- For consistency with verification, alleviation of some objectives

3	Software architecture is developed.	5.2.1.a	5.2.2.a 5.2.2.d	○	○	○	○	Design Description	11.10	①	①	①	②
4	Low-level requirements are developed.	5.2.1.a	5.2.2.a 5.2.2.e 5.2.2.f 5.2.2.g 5.2.3.a 5.2.3.b 5.2.4.a 5.2.4.b 5.2.4.c 5.5.b	○	○	○	<del>○</del>	Design Description	11.10	①	①	①	
								Trace Data	11.21	①	①	①	
5	Derived low-level requirements are defined and provided to the system processes, including the system safety assessment process.	5.2.1.b	5.2.2.b 5.2.2.c	○	○	○	<del>○</del>	Design Description	11.10	①	①	①	
6	Source Code is developed.	5.3.1.a	5.3.2.a 5.3.2.b 5.3.2.c 5.3.2.d 5.5.c	○	○	○	<del>○</del>	Source Code	11.11	①	①	①	
								Trace Data	11.21	①	①	①	

# 3- A new release: Impact

## Objectives: Verification of additional code (Level A)

- Source code/object code traceability aspect translated into a new objective in table A-7

9	Verification of additional code, that cannot be traced to Source Code, is achieved.	6.4.4.c	6.4.4.2.b	●				Software Verification Results	11.14	②			
---	---	---------	-----------	---	--	--	--	-------------------------------	-------	---	--	--	--

# 3- A new release: Impact

## Objectives: SQA objectives

**Table A-1 Software Planning Process**

	Description	Ref.	A	B	C	D
6	Software plans comply with this document.	4.1f 4.6	○	○	○	
7	Software plans are coordinated.	4.1g 4.6	○	○	○	



**TABLE A-9  
SOFTWARE QUALITY ASSURANCE PROCESS**

	Objective	Ref	Activity Ref	Applicability by Software Level			
				A	B	C	D
1	Assurance is obtained that software plans and standards are developed and reviewed for compliance with this document and for consistency.	8.1.a	8.2.b 8.2.h 8.2.i	●	●	●	
2	Assurance is obtained that software life cycle processes comply with approved software plans.	8.1.b	8.2.a 8.2.c 8.2.d 8.2.f 8.2.h 8.2.i	●	●	●	●
3	Assurance is obtained that software life cycle processes comply with approved software standards.	8.1.b	8.2.a 8.2.c 8.2.d 8.2.f 8.2.h 8.2.i	●	●	●	
4	Assurance is obtained that transition criteria for the software life cycle processes are satisfied.	8.1.c	8.2.e 8.2.h 8.2.i	●	●	●	
5	Assurance is obtained that software conformity review is conducted.	8.1.d	8.2.g 8.2.h 8.3	●	●	●	●

+ Independence

+ Transition criteria for level C

## 3- A new release: Impact

- Errors:
- Consistent terminology
- Clarifications
- Hidden Objectives
- New topics
  - Aspects not (enough) addressed
  - May come from some CRI or others documents

**May have an (limited) impact!**

# 3- A new release: Impact

**New topics:** Assessment of tool known errors ( § 4.4.1)

f. Known tool problems and limitations should be assessed and those issues which can adversely affect airborne software should be addressed.

Known problems should be

1- available

2- assessed for possible impact on software

*Scope: Same as for item e, so "especially for compilers and auto-code generators"*

# 3- A new release: Impact

**New topics:** Parameter Data Item with related objectives and activities

Purpose: To make possible:

- To verify the software without knowing the final (or multiple) values of PDI
- To change the values of PDI without re-enter software verification

# 3- A new release: Impact

**New topics:** Items added “*accuracy and consistency of source code*”

f. Accuracy and consistency: The objective is to determine the correctness and consistency of the Source Code, including stack usage, memory usage, fixed point arithmetic overflow and resolution, floating-point arithmetic, resource contention and limitations, worst-case execution timing, exception handling, use of uninitialized variables, cache management, unused variables, and data corruption due to task or interrupt conflicts.



# 4- Other documents

**Ground based software (CNS/ATM) (DO-278A/109A)**

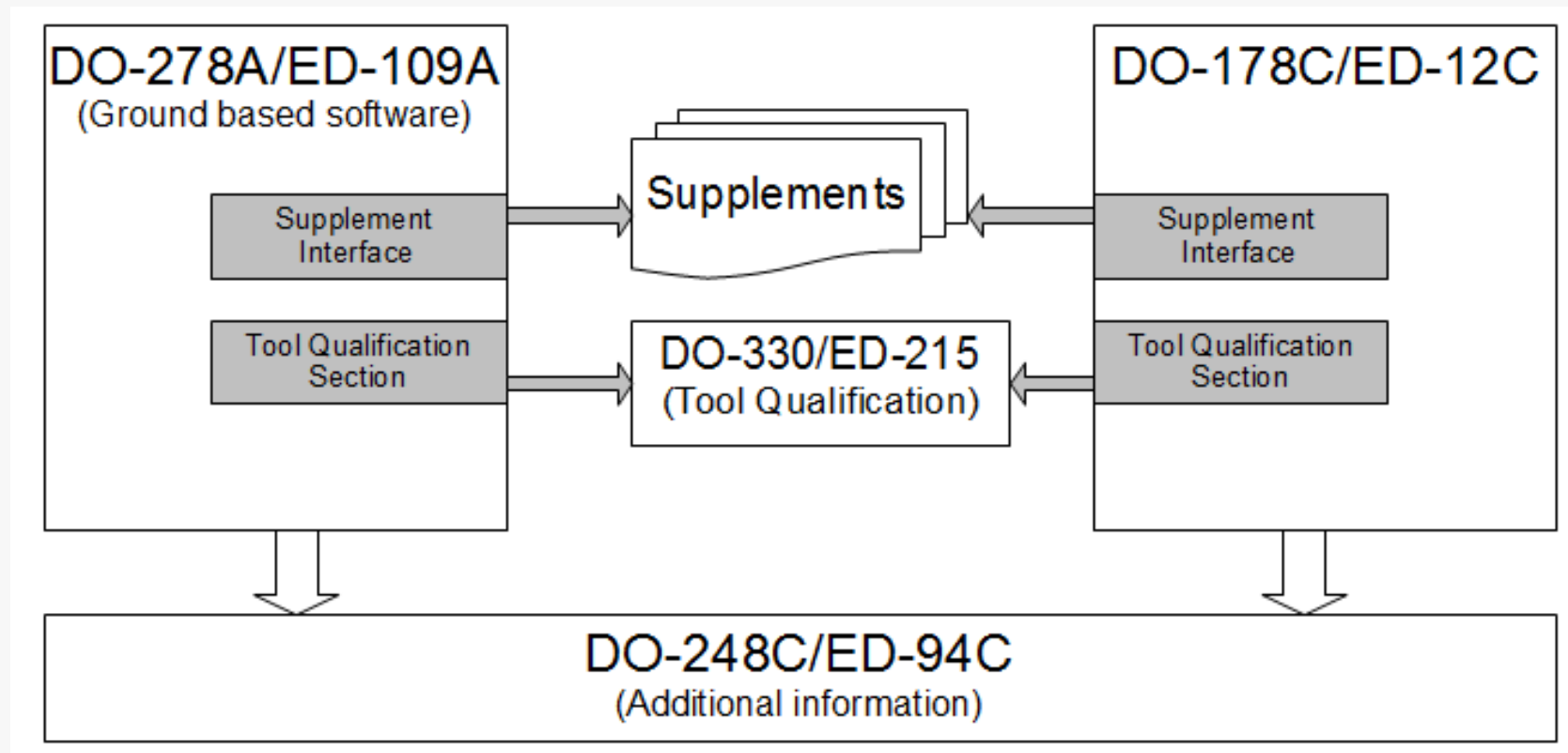
**Tool Qualification Document (DO-330/ED-215)**

## **3 Supplements:**

- Model Based Development and Verification DO-331/ED-218
- Object Oriented Technologies and Related Techniques DO-332/ED-217
- Formal Methods DO-333/ED-216

**Supporting Information (DO-248C/ED-94C)**

# 4- Other documents



# 4- Other documents

## What is a supplement ?

- Address a specific method/technology
- Extend the core document for this method/technology
- Provide characteristics, used as basis for guidance
- May add, delete or modify from the core document:
  - Objectives
  - Activities
  - Life cycle data
- May provide supporting information

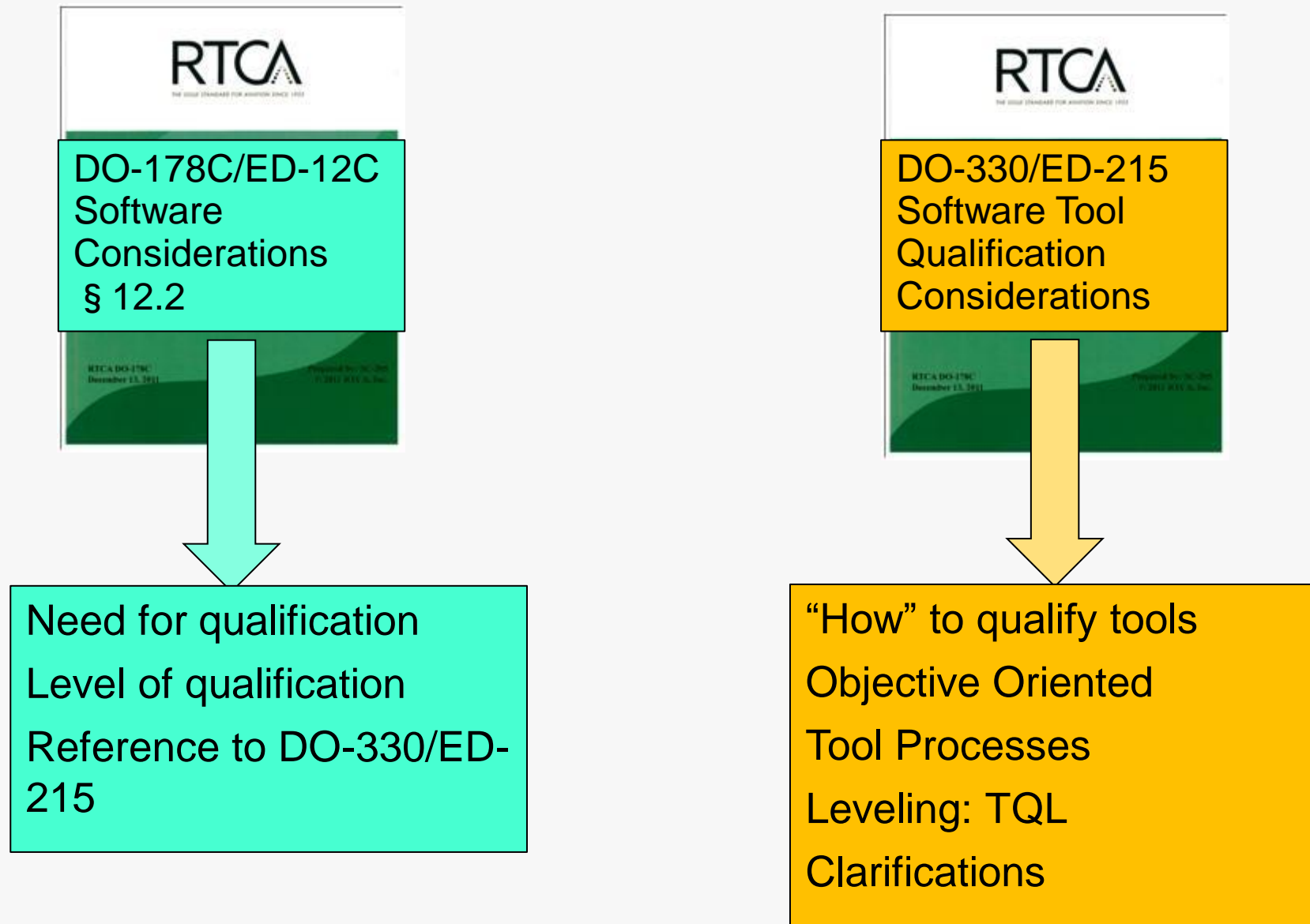
## 4- Other documents

**What is a supplement ?**

A supplement cannot be used  
separately from the DO-  
178C/ED-12C

# 4- Other documents

**A new tool qualification document, multi-domain, stand-alone**





A lot of work, almost 8 years  
discussion .... Worth the cost?

**Consensus** n. Collective opinion or concord; general agreement or accord. [Latin, from *consentire*, to agree]

# 5- FAS for the future

## **WG71/SC205 Way of life:**

Term of references initially “disallowed” changes

“Dinosaurs”: “*DO-178B is perfect, no need for change*”

Low level of expertise (FAA DER, “pseudo-consultants” ....)

Low representation of experts in some domain and few background of using new methods/technics

Turn over, number of comments (*up to 150 attendees in conferences, and more than 1000 people registered on web site, provided comments*)

Need consensus for text approval

**=> *Better preparation for the future is necessary***

# 5- FAS for the future

## *Forum on Aeronautical Software (FAS)*

FAS shall **monitor** and **exchange information** on the application of the RTCA/EUROCAE “software document suite”:

Launched in 2012 by RTCA and EUROCAE



# 5- FAS for the future

## ***Forum on Aeronautical Software (FAS) : Main Goals***

- To share lessons learned in the use of the documents
- To identify and record any issues or errata showing the need for modifications to the “software document suite”.
- To develop and revise Frequently Asked Questions and Information Papers (IPs) for clarification

However, for “official changes”

- “software document suite”,
- a new technology supplement

the FAS will ask RTCA/EUROCAE and FAA/EASA to create a new Working Group.

# 5- FAS for the future

## *Forum on Aeronautical Software (FAS) : Products*

- Information Papers (IPs): Not official policy or position from RTCA/EUROCAE or any regulatory agency or authority.
- Made available (where ????)
- For educational and informational purposes only.



# 5- FAS for the future

## *Forum on Aeronautical Software (FAS) : Membership*

**Not an open group!**

Membership limited to

- Executive Management Committee
  - US and European Chairmen and Secretaries
  - FAA/EASA representatives
  - EUROCAE/RTCA representatives
- FAS Members: Mainly WG71/SC205 Subgroup chairs + coopted members

# 5- FAS for the future

***Forum on Aeronautical Software (FAS) : Membership***

**Not an open group!**

**But we encourage YOU to send your comments to us !**