aeroconseil
AKKA TECHNOLOGIES GROUP

Les points clés et les évolutions de la certification avionique ED-80 / DO254 (Hardware)

Etat des lieux

Perspectives d'évolution de la réglementation

AVIATION ENGINEERING & SERVICES
aeroconseil
AKKA TECHNOLOGIES GROUP

Rédacteurs du document ED-80 / DO- 254

- Aircraft manufacturers (Airbus, Boeing, Dassault, Embraer, Bombardier …..)
- Equipementters majeurs Main Avionics suppliers
- Autorités de certification
- Agence Spatiale : NASA

Released in April 2000

Joint Document :
EUROCAE (ED80) / RTCA (DO254)

Quelques notions clés

Le standard est rédigé de façon <u>générique</u>

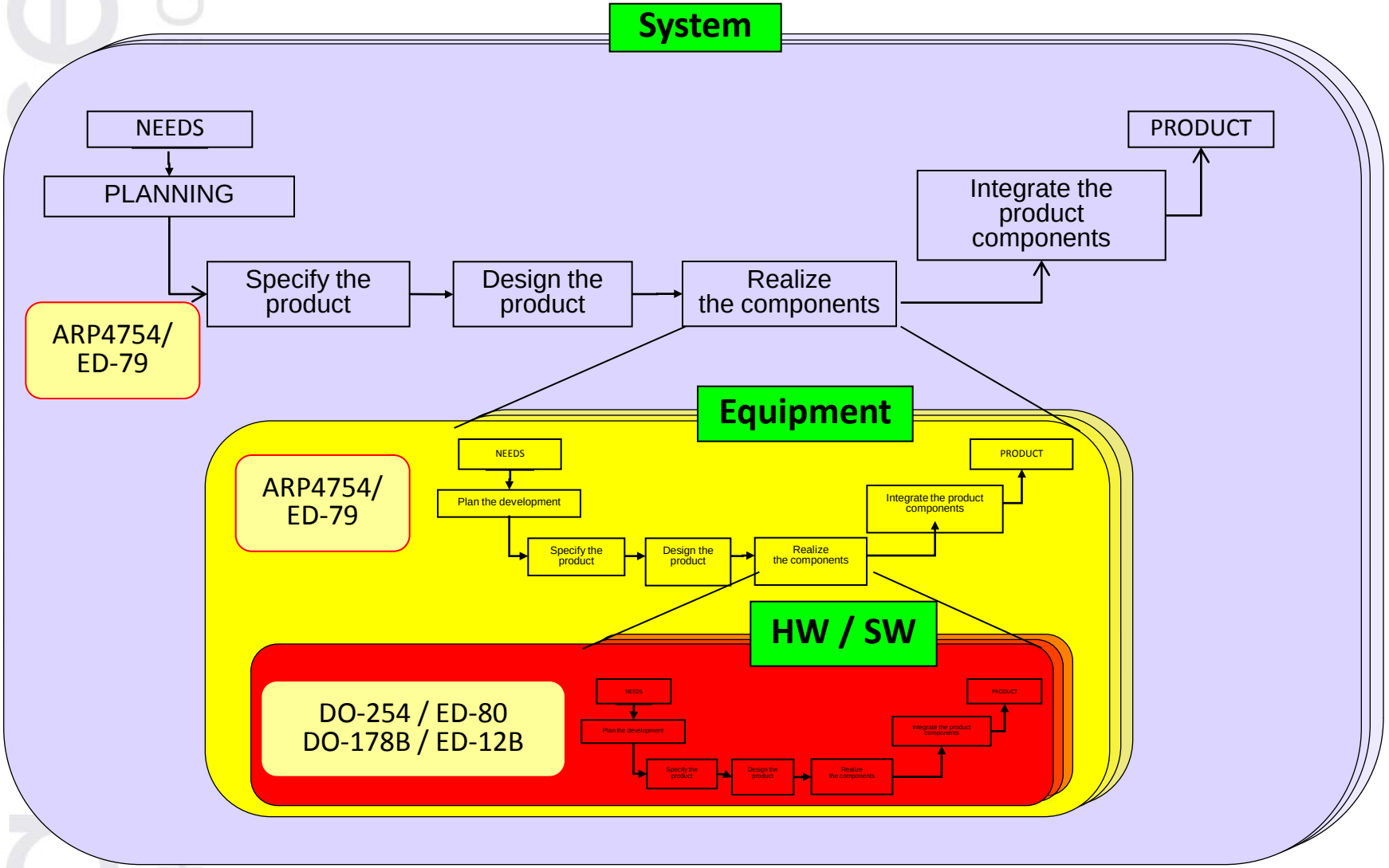
- Définit des objectifs et données à produire, pas une solution (process industriel, outils,…),
- C'est à l'industriel de faire ses choix, de les justifier et de démontrer leur conformité par rapport aux objectifs.

Basé sur un <u>processus structuré</u>

- Définition de phase en termes d'activités, de moyens, d'entrées-sorties, et de critères de transition entre phases
- Des activités transverses applicables à toutes les phases :
  - Vérification & Validation, Process Assurance, Gestion de Configuration & Gestion des changements, Liaison avec les Autorités.

Le niveau de criticité (DAL) impacte les activités à réaliser et la documentation à produire.

Quelques notions clés



Quelques notions clés

Approche Top-Down, orientée exigences

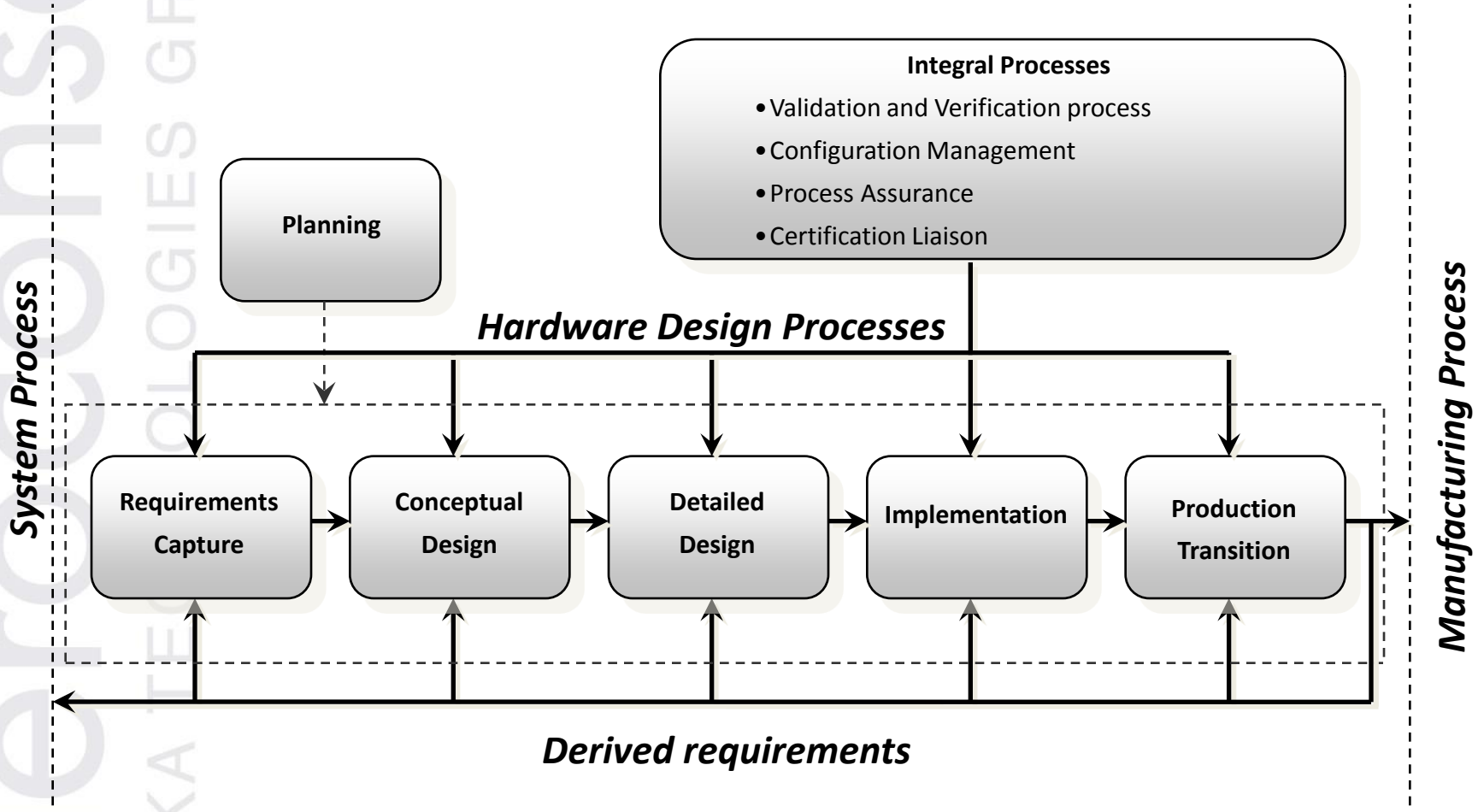
- Les exigences sont clairement identifiées.
- Le développement et la V&V sont réalisées en regard de ces exigences, avec une traçabilité démontrable.
- Cette approche implique donc une gestion particulière des cas basés sur un existant : Reuse, IP, COTS,…

Tool Assessment & Qualification

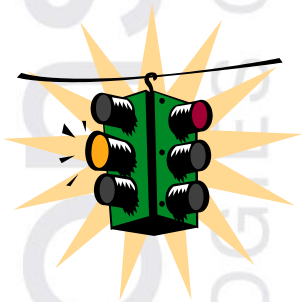
- Aucune confiance n'est accordée a priori aux outils
- La confiance est acquise soit par :
  - Une vérification indépendante des sorties de l'outil
  - Une expérience en service significative et démontrable
  - Des activités spécifiques de caractérisation de l'outil.

Ecrire ce qu'on va faire
Faire ce qu'on a écrit (ou maîtriser les écarts)
Justifier que ce qui est fait répond aux objectifs.

Cycle type DO-254



Résumé des processus DO254



Planning

- Un projet démarre par une phase de Planning (≠ calendrier !!)
- Des “Plans” sont rédigés avant le démarrage du projet, pour présenter les activités, les stratégies, les outils utilisés, les points particuliers et démontrer la conformité aux objectifs,
- Ces plans sont un support aux échanges avec les Autorités
- Ils doivent aussi être rédigés pour être utiles au projet, et suivis !
- **Plan clé en contexte DO254 = Le PHAC** (Plan for Hardware Aspects of Certification)
- Autres Plans : Development Plan, V&V Plan, Configuration Management plan, Process Assurance Plan

Résumé des processus DO254

Requirements Capture

- Identifier de façon formelle les exigences du produit.

Conceptual Design

- En général ce sont les premières phases de l'architecture

Detailed Design

- En général c'est le niveau du code VHDL.

Implémentation

- Cela correspond à obtenir un produit physique à partir des éléments de conception. Par exemple pour un FPGA, ce sont les activités de synthèse, placement routage et programmation du composant

Résumé des processus DO254

Production Transition

- Ce sont les activités permettant de reproduire en série le produit développé et vérifié (dossier de fabrication,…).

Validation

- S'assurer que les exigences sont **correctes** et **complètes**
- En général, revues. La traçabilité des exigences est utilisée également pour revoir les exigences par rapport au besoin exprimé au niveau supérieur

Vérification

- S'assurer que le produit répond à ses exigences
- En général, tests + traçabilité tests / exigences
- **L'indépendance est requise pour les activités de V&V sur les niveaux les plus critiques (A et B)**

Résumé des processus DO254

Gestion de configuration

- S'assurer que les données du cycle de vie produit sont correctement gérées en relation avec la version du produit et sa décomposition en sous-ensembles
- Définition de **baselines** pour figer les données (les exigences, les constituants techniques du produit à vérifier avant d'entrer en phase de tests,…)
- La gestion de configuration intègre la gestion des changements :
  - Capture des problèmes en « Problem Reports »
  - Analyse de l'impact du problème, des besoins de modification et de revérification

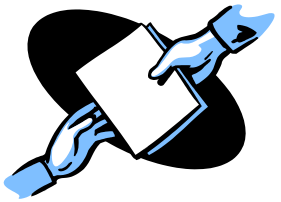
Résumé des processus DO254

Process Assurance

- Correspond à « l'assurance Qualité »
- S'assurer au travers d'audits ou revues que les processus décrits dans les plans sont respectés par les équipes techniques
- Détecter les écarts, suivre les actions correctives

Certification Liaison

- Echanges avec les Autorités de certification : fourniture des documents demandés (plans,…), audits,...



aeroconseil

AKKA TECHNOLOGIES GROUP

Constat sur le document ED-80 / DO-254

Constat sur le document ED-80 / DO-254

Certaines incohérences et omissions, technologies HW émergeantes non adressées

Exemples :

- Définition des critères de classification simple/complexe
- Définition d'indépendance
- Modifiable aspects of AEH devices
- Critère de couverture de code
- Robustesse en vérification
- Single Event Effects
- Multicore processors
- …

EASA Certification Memos (CM)

L'EASA a rendu public plusieurs "Certification Memos":

- En 2011, 2 CM (1 SW & 1AEH) ont été publiés avec prise en compte des remarques du monde industriel: http://easa.europa.eu/certification/certification-memoranda.php

- Applicable à tout avionneur ou motoriste sollicitant l'approbation de l'EASA pour un produit (AEH aircraft, engine)

En pratique et dans la plupart des contextes :

- Les CRIs restent la référence et contiennent
  - Soit le CM "as is",
  - Ou bien le CM négocié, qui se traduit par un IM contenant les conclusions des discussions

CAST paper #31 (PP-31)

« Technical Clarifications for RTCA DO-254 / EUROCAE ED-80 “

- identifie les erreurs, les omissions, les sujets obsolètes et tout autre clarification nécessaire au document ED-80/DO-254
- Publié en Décembre 2012 : **Download Link**

Faut-il éditer une nouvelle version du document ED-80 / DO-254 ?

aeroconseil

AKKA TECHNOLOGIES GROUP

Reopening ED-80/DO-254 ?

Reopening ED-80 / DO-254… ?

Question d'actualité due

- à la date de publication du document (2000),
- aux révisions de l'ARP-4754A et du DO-178C,
- à l'évolution des technologies Hardware,
- aux ambigüités, différentes priorités et interprétations des autorités de certification …

Options to Develop COTS AEH Guidance

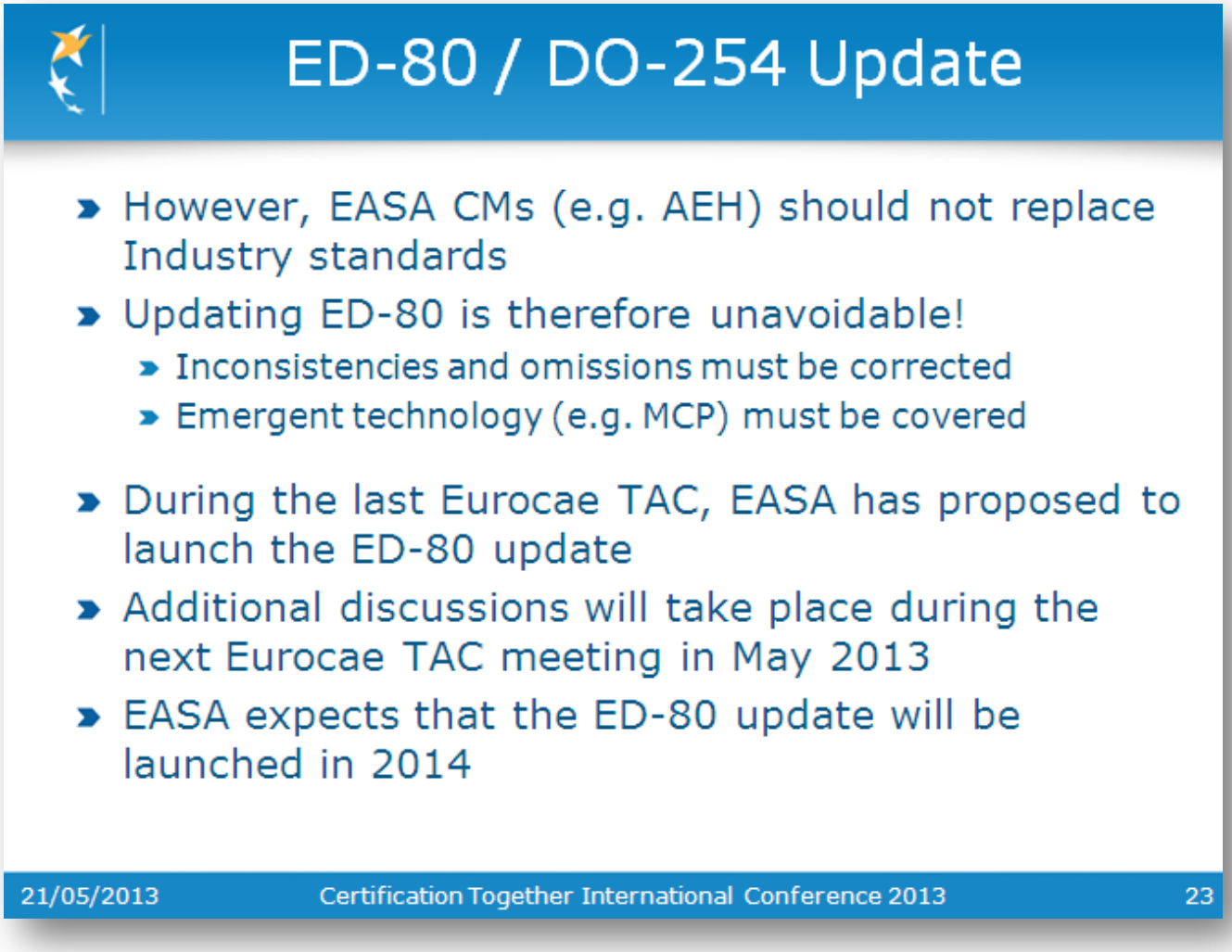
- Options to develop new COTS AEH guidance include:
  - (1) Revise RTCA DO-254
  - (2) Publish new RTCA DO standard
  - (3) Publish new advisory circular without a RTCA DO standard
  - (4) Publish Issue Papers

CAST PP-31 Next Steps

- Address PP-31 findings and recommendations
  - ✓ FAA working group to establish a list of priorities and schedule
  - ✓ Coordinate recommendations with CAST
  - ✓ Revise training materials as deemed necessary
  - ✓ AEH / SW team to provide recommendations on revising:
    - AC 20-152 (Only) to incorporate guidance from Order 8110.105 Change 1 and EASA CM-SWCEH-001, draft planned for FY-14
    - Revise DO-254 followed by an additional revision to AC 20-152
- Use research conducted by AVSI as input into FAA policy on COTS
  - ✓ COTS Intellectual Property (IP)
  - ✓ COTS issues in general

CTIC 2013 : position EASA

Le CM a pour objet de clarifier et de compléter plusieurs points



CTIC 2013 : présentation EASA

An EASA Concern: MCP

- EASA has concerns about a safe usage of MCP (MultiCore Processor)
- The Industry Group called MCFA has been created 3 years ago (MCFA: MultiCore For Avionics)
- During the last MCFA meeting (last January 13), EASA and the FAA got very fruitful discussions with the Industry
- A preliminary consensus has been reached: generic CRI
- Additional feedback is expected in 2013 and MCP policy could possibly be introduced in the revised AEH CM in 2014
- Challenge: MCP technology develops very fast

Coordination with other Authorities

- Coordination with other Authorities and particularly the FAA (e.g. AMC/AC 20.115C) :
  - Regulations and Guidance Material cannot be identical line by line (as for any other rule: Part 21, CS/FAR 25, etc.)
  - Additional guidance material like FAA Orders, FAA policy Memos, Cert. Memos, CAST Papers, etc. are therefore used to ensure global coordination between Authorities

DO254 User Group discussions

En 2013, discussions au sein du DO254 User Group Europe.

Consensus sur : "*Why Re-opening the DO-254 ?*

- *Harmonization of certification requests between EASA / FAA / other authorities*
- *Opportunity to capture industry position in a standard*
- *Consensus on certification requests between EASA/FAA & Industry*
- *Common baseline on certification requests on all aircrafts and equipments*
- *Gaps / Obsolescence of some parts of DO-254*
- *Clarifications & modulation according to the level considered (LRU, Board, PLDs)*
- *Include technology evolutions (since 2000)/ unavoidable COTS usage (IP, devices…)*
- *Harmonize DO-254 with ARP-4754A*"

DO254 User Group discussions

“Conditions for reopening

- *EASA & FAA participation for recognition of updated document*
- *Creation of Eurocae/RTCA working with approved Terms Of Reference*
- *Taking into account lessons learned from DO-178C regarding to group management, decision process, group size, rules for participation…*
- *Keep an objective–oriented document*
- *Retain but refine/clarify the existing DO-254 objectives*
- *Avoid/minimize impact on existing DO-254 compliant industrial processes*
- *Focus and limit scope on pre-agreed topics*
- *The output shall be a DO-254A treating all Hardware aspects”*

aeroconseil
AKKA TECHNOLOGIES GROUP

Merci pour votre attention,

Questions ?

AVIATION
ENGINEERING
& SERVICES
aeroconseil
AKKA TECHNOLOGIES GROUP