Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

Evolutions des standards aéronautiques

laurent.plateaux@dga.defense.gouv.fr
jean-françois.sicard@dga.defense.gouv.fr
DGA Techniques aéronautiques

DGA

DIRECTION GÉNÉRALE DE L'ARMEMENT

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ED-79/ARP-4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

V. Les évolutions de la DO-160

VI. Les aspects Air Traffic Management

VII. La navigabilité des aéronefs militaires et d'Etat

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ED-79/ARP-4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

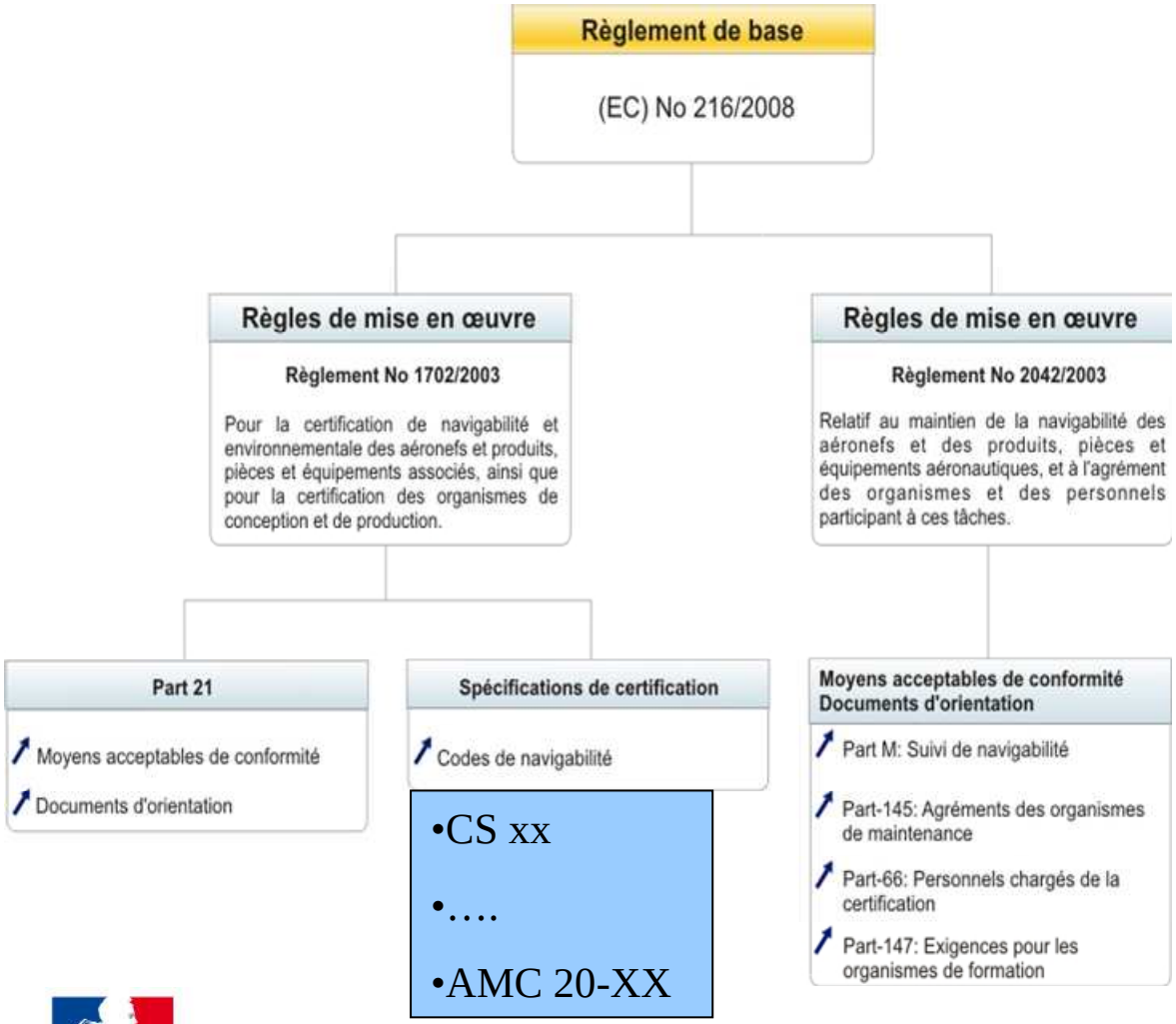
V. Les évolutions de l'ED-14/DO-160

VI. Les aspects Air Traffic Management

VII. La navigabilité des aéronefs militaires et d'Etat

L'Agence Européenne de la Sécurité Aérienne

http : //www.easa.europa.eu



Le règlement EC 216 /2008 précise les missions de l'EASA et les exigences essentielles en matière de navigabilité.

Le règlement EC 1702/2003 définit les exigences techniques et procédures administratives pour la certification de navigabilité et environnementale des produits et des pièces.

L'EASA et la FAA établissent en coordination les spécifications de certification qui sont déclinées par type d'aéronefs:

- CS-25 (large aircraft)
- CS-29 (large rotorcraft)
- CS-E (engines)
- …

La notion de risque aéronautique

- Les statistiques mondiales donnent toutes causes confondues un taux moyen d'accident mortel de un par million d'heures de vol.
- Un accident catastrophique sur 10 est imputable à l'avion; au niveau avion, la probabilité tolérée de catastrophe est d'au plus 10^{-7} par heure de vol.
- En moyenne, une centaine de pannes catastrophiques indépendantes imputables aux systèmes sont recensées au niveau avion → 100*P_systèmes < 10^{-7};

10^{-9} catastrophic failure conditions / flight hours is the objective to be respected for critical systems

+ fail-safe concept: any single failure can't lead to a catastrophic failure condition

Catégories de pannes

Allowable Qualitative Probability	No Probability Requirement	<---Probable---->	<----Remote---->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect	<-----Minor----->	<-----Major----->	<--Hazardous-->	Catastrophic
Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.					

c. The safety objectives associated with Catastrophic Failure Conditions, may be satisfied by demonstrating that:

(1) No single failure will result in a Catastrophic Failure Condition; and

(2) Each Catastrophic Failure Condition is Extremely Improbable.

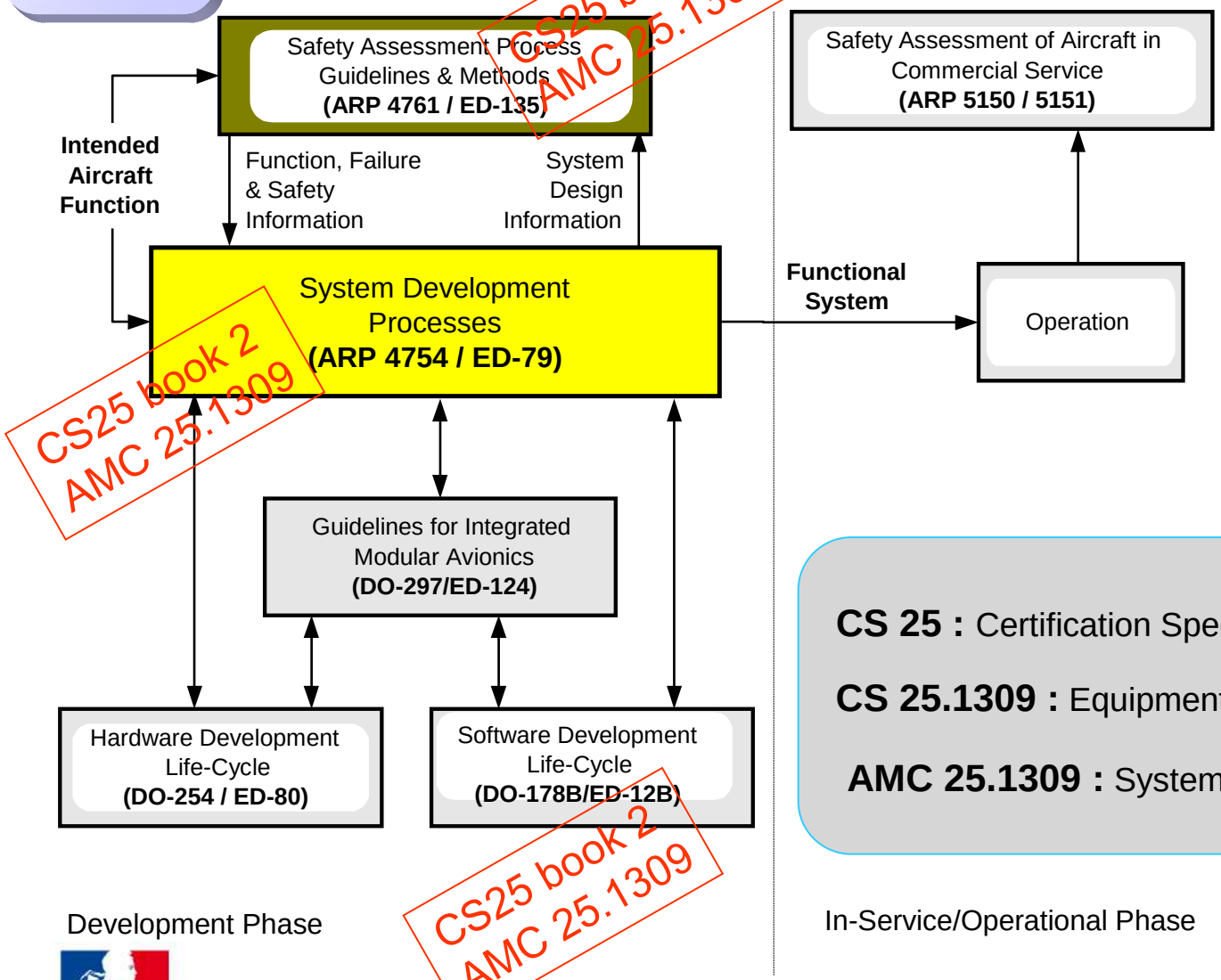
d. Exceptionally, for paragraph 8c(2) above of this AMC, if it is not technologically or economically practicable to meet the numerical criteria for a Catastrophic Failure Condition, the safety objective may be met by accomplishing all of the following:

(1) Utilising well proven methods for the design and construction of the system; and

La CS25.1309 introduit la notion de relation inverse entre probabilité d'occurrence et gravité des conséquences.

Failure Condition→ A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

Les relations entre les standards



Airworthiness standards for Safety

CS 25 : Certification Specifications for Large Aeroplanes

CS 25.1309 : Equipment, Systems & Installations

AMC 25.1309 : System Design & Analysis

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ED-79/ARP-4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

V. Les évolutions de l'ED-14/DO-160

VI. Les aspects Air Traffic Management

VII. La navigabilité des aéronefs militaires et d'Etat

ED-79/ARP-4754 : Objectifs

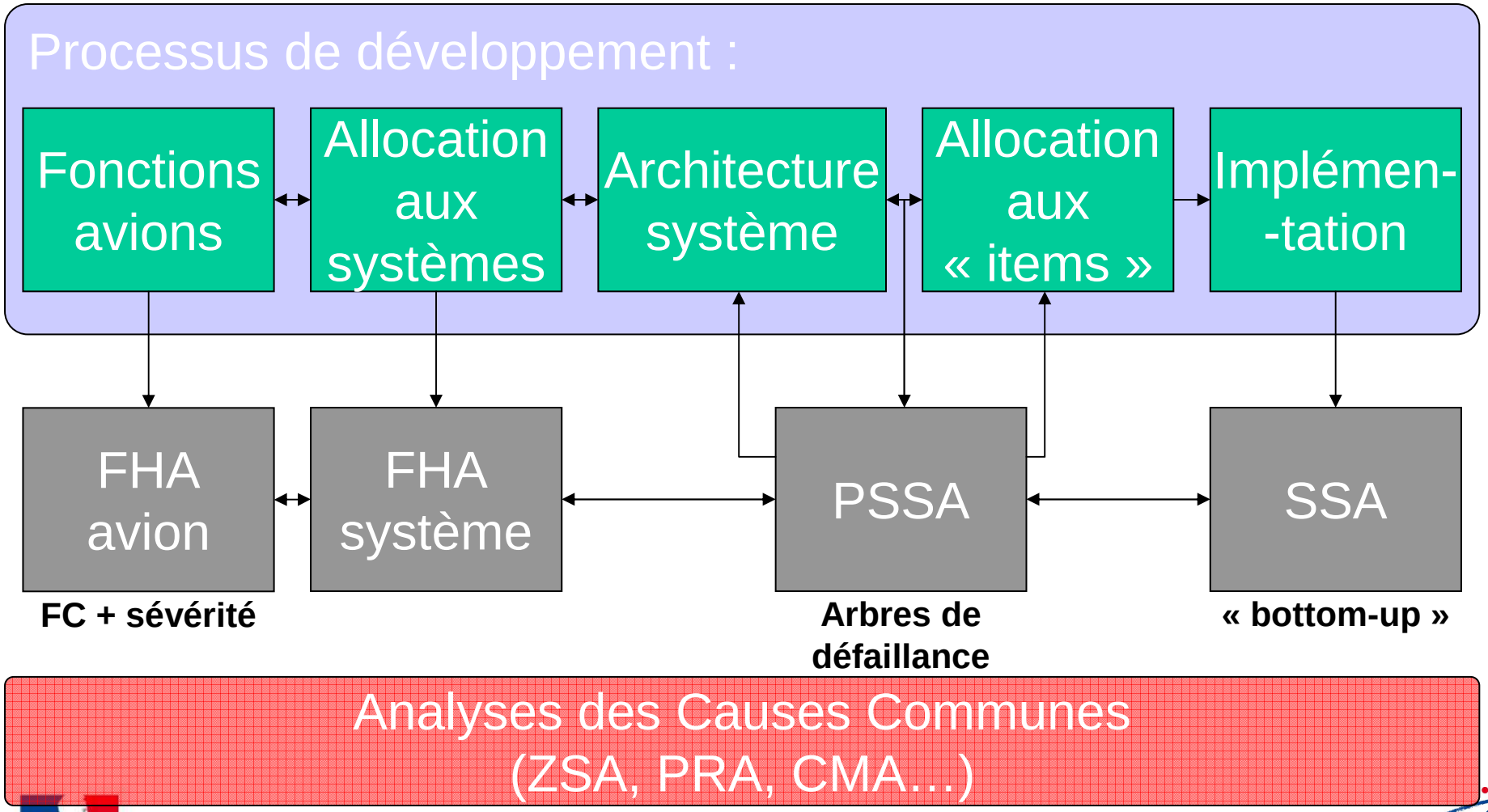
- **Le développement d'un aéronef**
  - D'un « concept » à une architecture de systèmes
  - Des risques pour la sécurité portés par chaque élément
  - Une complexité à maîtriser en vue de garantir la sécurité

- **Il faut guider le développement pour démontrer la satisfaction aux exigences de navigabilité.**

- **Deux exigences :**
  - Démontrer la tenue de l'architecture sélectionnée aux taux de pannes acceptables
  - Démontrer l'absence (ou le confinement) des erreurs qui auraient pu être introduites durant le développement

- **Comment ?**
  - Calculs des probabilités d'occurrence des pannes → analyses quantitatives
  - Prévention (confinement) des erreurs de développement par la mise en place de l'ASSURANCE DE DEVELOPPEMENT → analyses qualitatives;

ED-79/ARP-4754 : Évaluer la sécurité

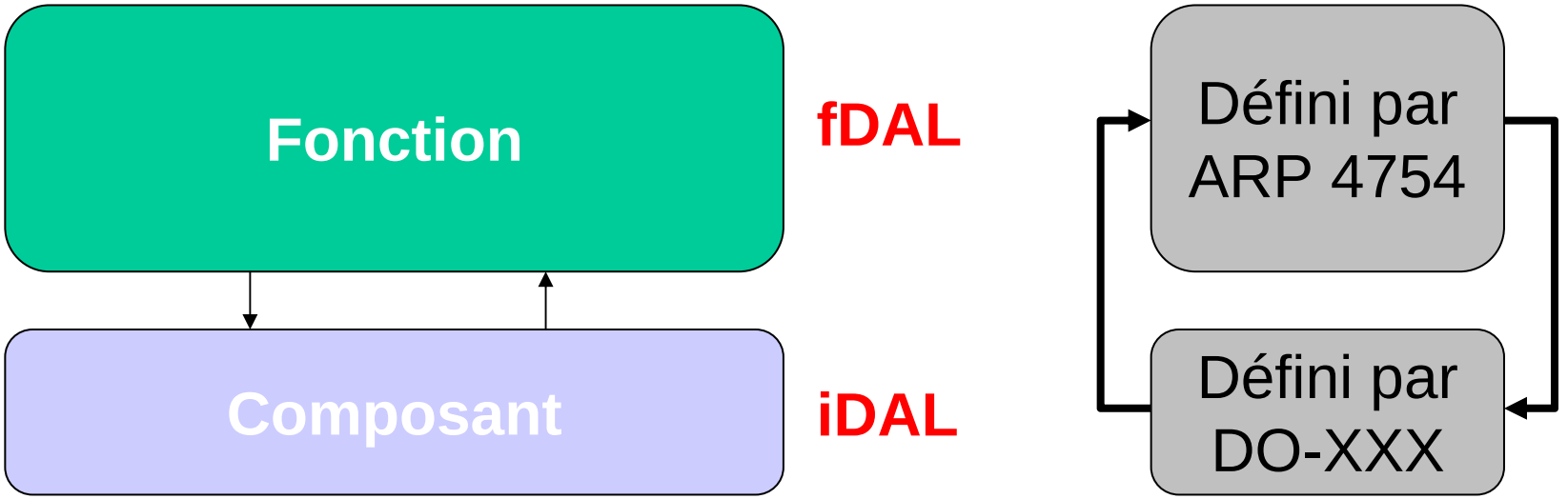


Evolution de l'ED-79/ARP-4754

- Le WG-63 de l'EUROCAE a mis à jour l'ED-79/ARP-4754 Pas d'évolution fondamentale mais une plus grande souplesse d'application.
- La nouvelle version privilégie une approche analytique basée sur une meilleure prise en compte des architectures : mise en place des fDAL et des iDAL.
- La mise à jour de l'ED-79/ARP-4754 est terminée.

L'assurance de développement

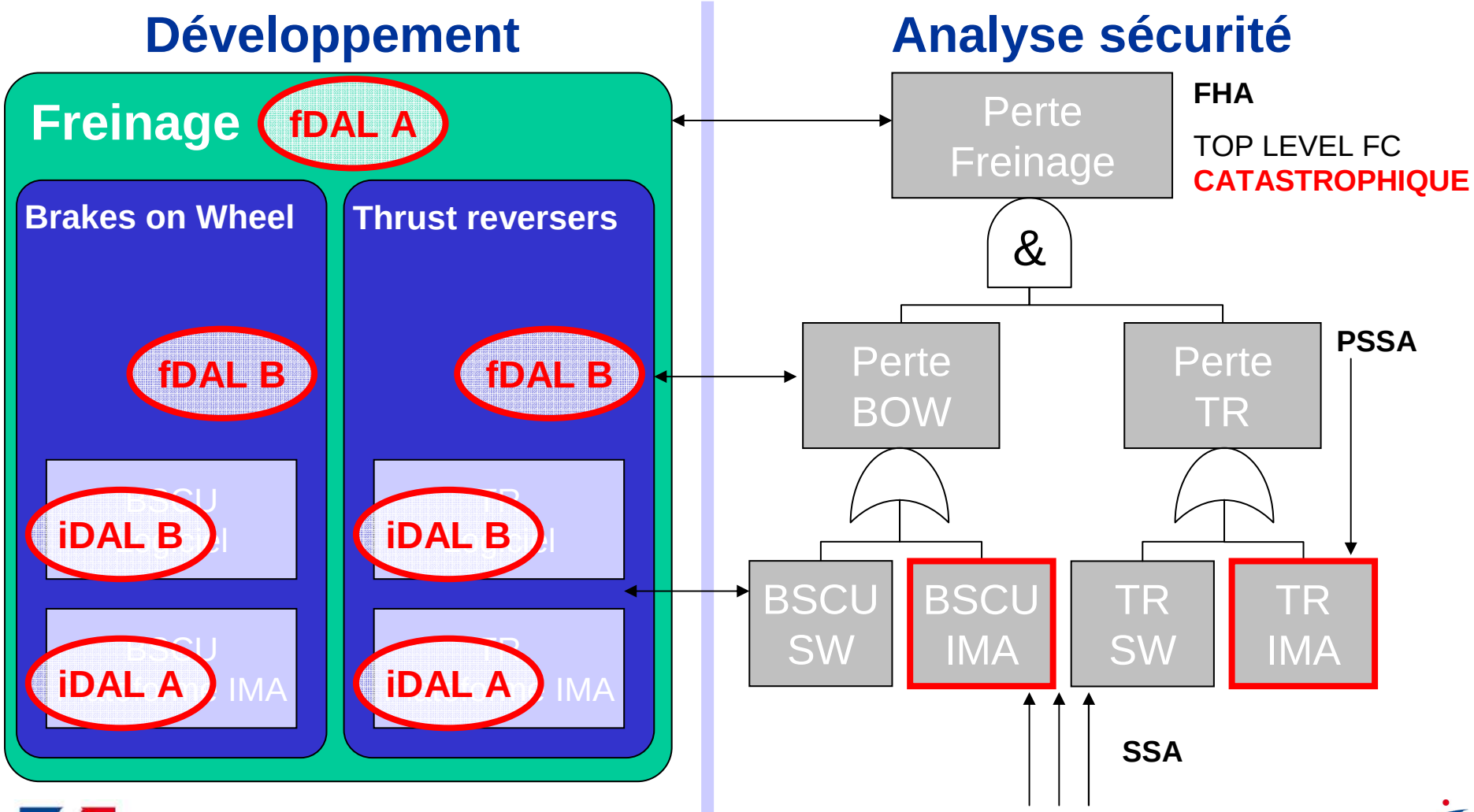
- On distingue deux types de niveaux d'assurance de développement :
  - fDAL : ***Function*** *Development Assurance Level*
  - iDAL : ***Item*** *Development Assurance Level*
- **Le niveau d'assurance de développement fait l'interface entre le système et le logiciel et les matériels électroniques complexes.**



Principe d'allocation des niveaux d'assurance de développement (DAL)

- Objectif :
  - Tirer profit des considérations d'architecture pour une allocation proportionnée du DAL
- Des postulats :
  - La rigueur doit être proportionnée par rapport à la sévérité des conditions de panne (5 niveaux de DAL)
  - On acceptera un développement conduit avec une rigueur moins grande si on fait le choix de la « dissimilarité »
- La FHA et la PSSA sont les points d'entrées du processus d'allocation des DAL
- Facteur essentiel : évaluer **les critères d'indépendances**
  - Indépendance des spécifications
  - Indépendance des choix de conception
- Le concept primordial : les ***Functional Failure Sets***

Principe d'allocation des DAL



Résumé des notions fondamentales

- Le fDAL contraint le développement des spécifications des systèmes
- Le iDAL fait le lien avec le développement des logiciels et des composants électroniques complexes
- Le principe d'allocation des DAL incite à faire des redondances indépendantes
  - Du point de vue fonctionnel
  - Du point de vue des choix de conceptions
- L'ED-79a/ARP-4754a est en cours d'approbation officielle

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ED-79/ARP-4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

V. Les évolutions de l'ED-14/DO-160

VI. Les aspects Air Traffic Management

VII. La navigabilité des aéronefs militaires et d'Etat

ED-12B / DO-178B : liens avec le système

- Software considerations in airborne systems and equipment certification

- Le niveau du logiciel est déterminé en fonction du DAL de la fonction à laquelle il contribue et en prenant en compte des considérations architecturales.

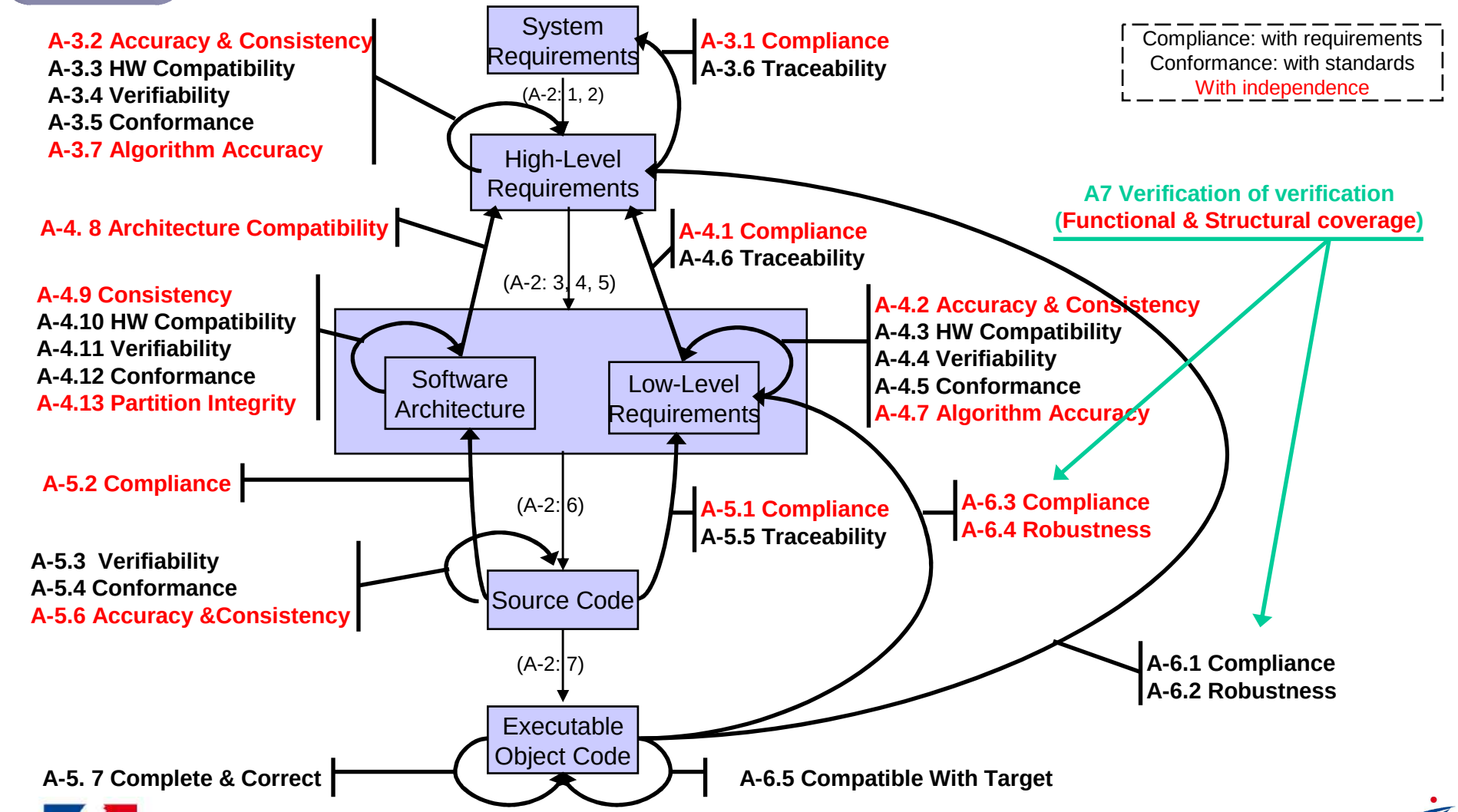
- Le développement du logiciel doit ensuite respecter les objectifs définis dans l'ED-12B / DO-178B ainsi que les Certification Review Item.
  - L'EASA a publié un « Cert Memo » logiciel : http://easa.europa.eu/certification/current-consultations.php dont la vocation est de servir de base à des futurs CRIs

Failure condition	fDAL	iDAL
CAT (10^{-9})	A	≤ A
HAZ (10^{-7})	B	≤ B
MAJ (10^{-5})	C	≤ C
MIN	D	≤ D
No safety effect	E	E

ED-12B : processus développement

- Développement des exigences
  - Développer les exigences de haut niveau logiciel (HLR) à partir des données du système.
- Développement de l'architecture et des exigences bas niveau
  - Développer l'architecture et les exigences de bas niveau du logiciel (LLR) à partir des exigences de haut niveau, des standards de conception et de choix techniques.
- Développement du code source
  - Implémenter le code source à partir des exigences de bas niveau et de l'architecture du logiciel.
- Intégration
  - Compiler et assembler le code source de façon à former un code objet exécutable téléchargeable sur la cible

ED-12B/DO178-B : vérification



Vers l'ED-12C/DO-178C

Mandat et structure du WG-71

- Le WG-71 a pour mission d'élaborer :
  - la version C de la DO-178/ED-12 (Airborne SW) ;
  - La version A de la DO-248 (FAQ pour l'ED-12C) ;
  - la version A de l'ED-109/DO-278 (CNS/ATM SW).

- Le WG-71 est composé de 6 sous-groupes :
  - SG1 : Document Integration
  - SG2 : Issues and Rationale Subgroup
  - SG3 : Tool qualification
  - SG4 : Model Based Design & Verification
  - SG5 : Object Oriented Technology
  - SG6 : Formal methods
  - SG7 : CNS/ATM & Safety

ED-12C/DO-178C : échéances et tendances.

- Idées directrices :
  - maintenir le même niveau de sécurité ;
  - proposer des recommandations en regards des nouvelles tendances et technologies, en particulier, feront l'objet d'un supplément (annexe) :
    - La conception/vérification basée sur les modèles,
    - Les technologies objet,
    - Les méthodes formelles.
  - Proposer une nouvelle DO dédiée à la qualification d'outils

- La rédaction a été finalisée fin 2010
- Processus « FRAC » - de fin 2010 à octobre 2010
- Acceptation par les autorités à partir d'octobre 2011

ED-12C/DO-178C : Changements de fond.

- Corps du texte : clarification, précisions, assouplissements
- Model based development : traduction de concepts de la DO aux langages de modélisation graphique des exigences, nouveaux concepts de couverture de tests, introduction de la simulation de modèle (non finalisé).
- Méthodes formelles : introduction des méthodes formelles comme méthode alternative aux revues, analyses et tests.
- Techniques Objet : propose une liste des vulnérabilités liées aux OOTs, des compléments et ajouts aux objectifs DO178 existants et des recommandations et des directives pour l'utilisation des ces technologies.

Nouvelle DO/ED sur la qualification d'outils.

- Le corps du texte de la DO178C/ED12C se limite a décrire quand et pourquoi on doit qualifier un outil

- Le comment est l'objet d'un document qui a cessé d'être un supplément pour devenir une DO à part entière
  - Précision des rôles : développeur d'outil, utilisateur d'outil
  - Séparation des données : développement d'outil, qualification d'outil : approche à la fois plus souple et plus rigoureuse
  - Considérations complémentaires : Outils COTS, Réutilisation, « historique en service », …

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ARP4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

V. Les évolutions de la DO160

VI. Les aspects Air Traffic Management

VII. La navigabilité des aéronefs militaires et d'Etat

ED-80/DO-254

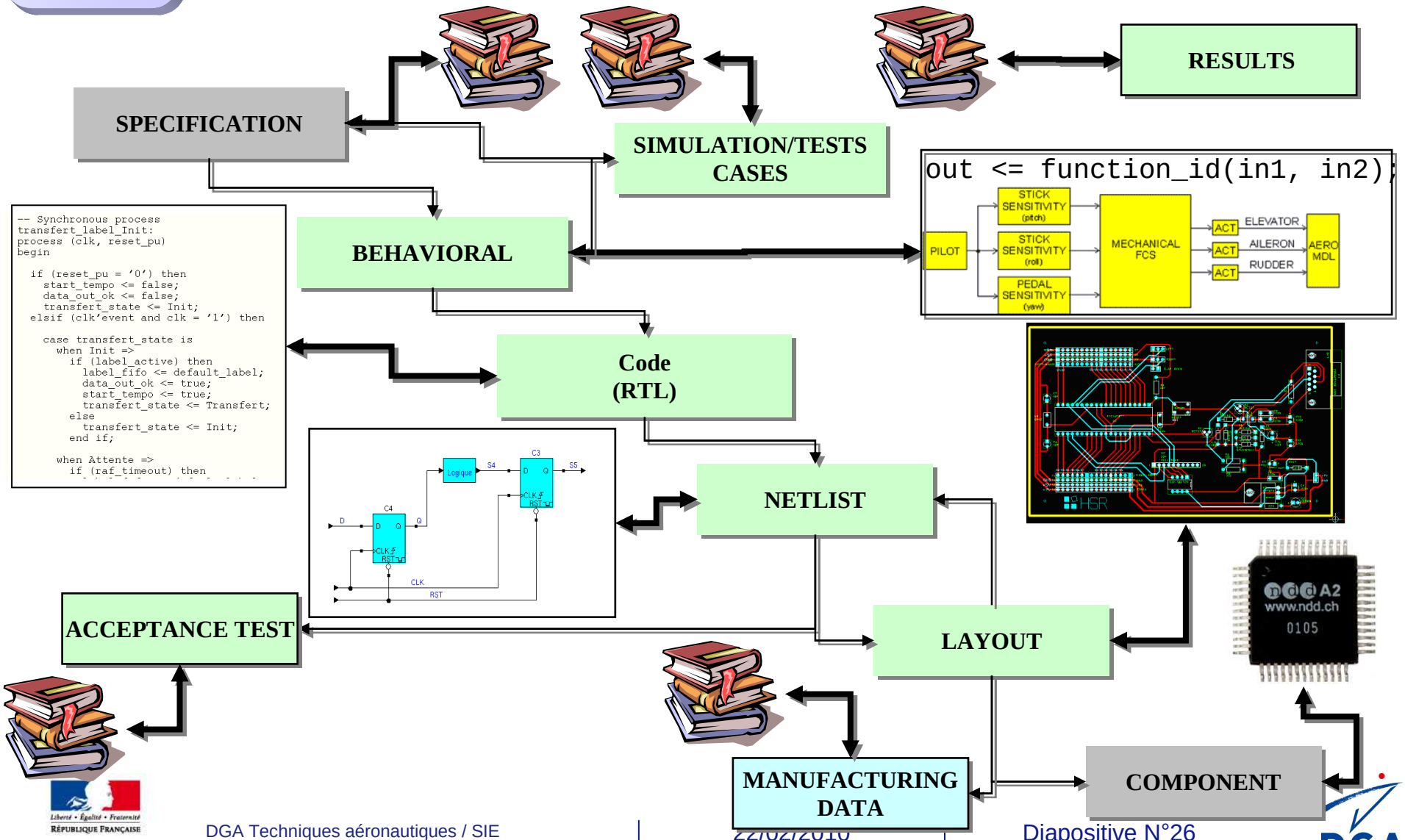
For each program, ED-80/DO-254 is made applicable for each Digital Device through *Certification Review Items* (CRIs)

Aircraft X *CERTIFICATION REVIEW ITEM*

Applicability	: Aircraft X	**Ref.**	:
Requirement	: *CS 25.1301&1309; SC A-1*	**Issue**	:
Advisory Material	: ED12B/DO178B, ED80/DO254	**Date**	:
Subject	: Digital Devices Design Assurance	**Status**	: *Closed*
Category	: Interpretative Material	**Next action by**	:
Primary	: Panel 10		
Secondary	: Panels 04, 05, 06, 07, 08		

The purpose of this Certification Review Item:
- issues additional considerations to use DO 254/ED-80 for certification aspects associated with Application Specific Integrated Circuits (ASICs) and Programmable Logic Devices (PLDs),
- Emphasises the use of DO 254 / ED80 for complex and digital Commercial Off-The-Shelf components, for systems containing digital electronics on the A/C X aircraft.

Les produits du cycle de vie



Les points clefs

- La cible de l'ED-80/DO-254 : L'électronique embarquée (un CRI peut limiter l'application aux composants électroniques complexes : ASICs, PLDs, FPGAs) ;
- Des niveaux de criticité sont définis comme pour le logiciel ;
- Classification simple / complexe (décision difficile basée sur des idées comme « un design est simple si il est 100% vérifiable », ce qui n'est pas d'une grande aide …) ;
- Outils de développement et de vérification : ils devraient être qualifiés;
- Traçabilité des exigences :
  - Requirements – Design traceability,
  - Requirements - Verification procedures and results traceability ;
- Vérification & Validation ;
- Problématique des COTS insuffisamment développée : nécessite des CRIs.

- L'EASA a publié un « Cert Memo » logiciel : http://easa.europa.eu/certification/current-consultations.php dont la vocation est de servir de base à des futurs CRIs

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ARP4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

V. Les évolutions de la DO-160

VI. Les aspects Air Traffic Management

VII. La navigabilité des aéronefs militaires et d'Etat

ED-14/DO-160 : conditions environnementales et procédures de tests d'équipements aéronautiques

- La dernière version en date est la version F (2007).
- La version G est en cours de rédaction et introduite des modifications liées à :
  - La prise en compte des Portable Electronic Devices
  - La prise en compte du GPS comme équipement de navigation primaire.
  - Le changement dans les essais de susceptibilité rayonnée : utilisation de chambres réverbérantes au lieu de chambres an échoïques.

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ED-79/ARP-4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

V. Les évolutions de l'ED-14/DO-160

VI. Les aspects Air Traffic Management

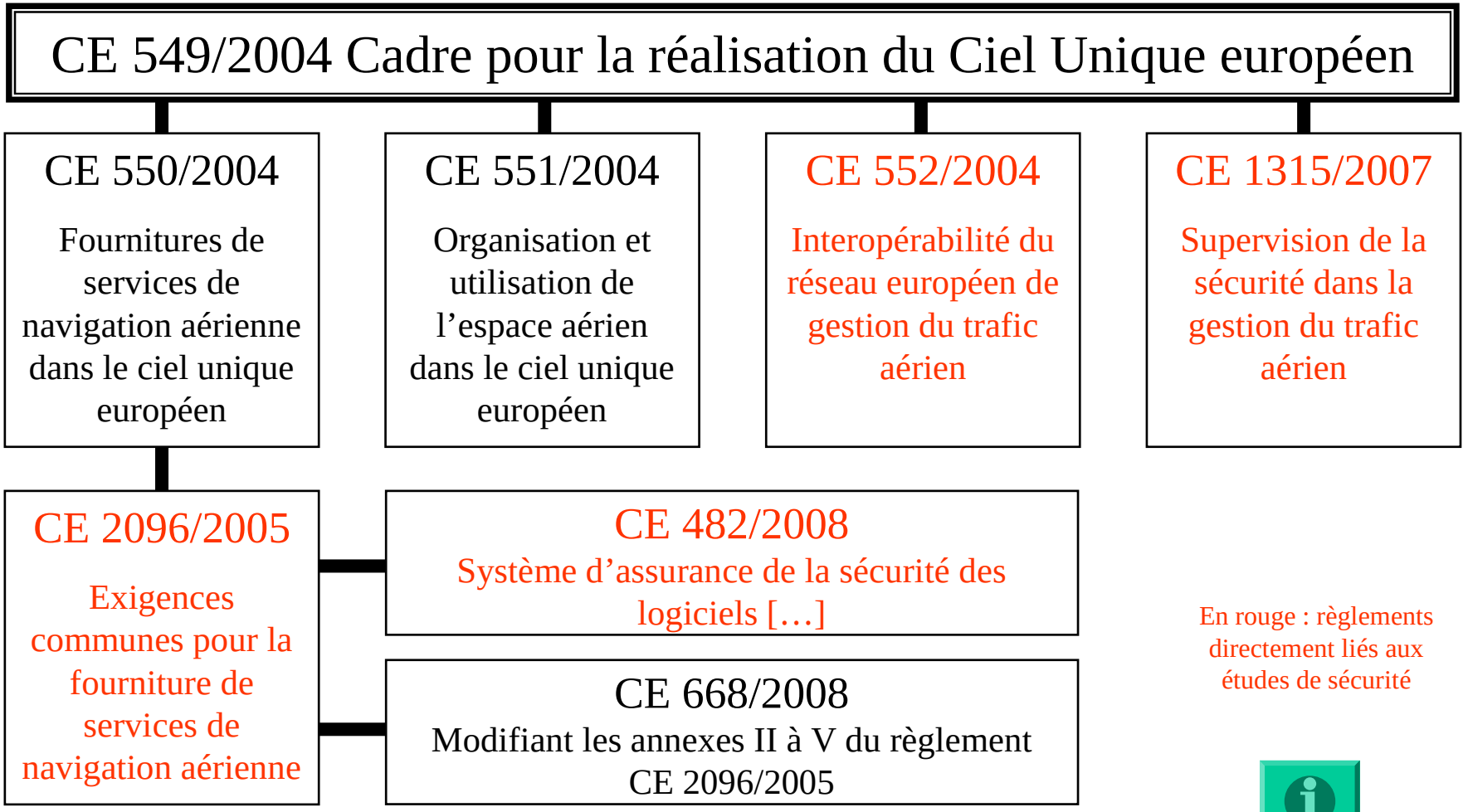
VII. La navigabilité des aéronefs militaires et d'Etat

Air Trafic Management : Règlements « Ciel unique I »

- Constitué par les règlements « Ciel Unique » de la commission européenne :
  - Ensemble de règlements CE, publiés depuis 2004
  - Directement applicables dans les 27 états membres de l'Union Européenne
    - Pas de « transposition » nécessaire en droit national
  - Applicables dans certains pays n'appartenant pas à l'UE (Suisse par exemple)
  - Basés sur les exigences réglementaires de sécurité d'Eurocontrol, ESARR (1 à 6), mais des différences de fond importantes existent : les ESARR ne sont plus le référentiel réglementaire français.

- Un règlement cadre : CE 549/2004

Air Traffic Management : Règlements « Ciel unique I »



En rouge : règlements directement liés aux études de sécurité

Plan de la présentation

I. La réglementation et les standards

II. Les processus d'évaluation de la sécurité; les évolutions de l'ED-79/ARP-4754

III. Vers l'ED-12C/DO-178C

IV. Présentation de l'ED-80/DO-254

V. Les évolutions de l'ED-14/DO-160

VI. Les aspects Air Traffic Management

VII. La navigabilité des aéronefs militaires et d'Etat

Navigabilité des aéronefs militaires et d'Etat (1/3)

- Publication fin 2006 des textes fondateurs :
  - 3 arrêtés fixant :
    - Les attributions de l'autorité technique (DGA) et des autorités d'emploi (utilisateurs Défense, Direction de la Défense et de la Sécurité Civiles et Direction Générale des Douanes et Droits Indirects) ;
    - Les règles d'immatriculation ;
    - Les conditions de délivrance, de maintien, de modification, de suspension ou de retrait des certificats de type ;
  - et 1 décret relatif aux règles d'utilisation, de navigabilité et d'immatriculation (**n° 2006-1551 du 7 décembre 2006)**

Nécessité de mise en place de l'ensemble des documents, procédures et organisations pour se mettre en conformité avec les textes réglementaires ci-dessus.

Navigabilité des aéronefs militaires et d'Etat (2/3)

- Orientations générales :
  - Permettre l'insertion des aéronefs militaires et d'état dans l'espace aérien civil ;
  - Coller le plus possible à la réglementation civile et mettre en œuvre les mêmes référentiels que pour les aéronefs civils :
    - Equivalent Part 21 (Exigences essentielles et FRA21),
    - ED-79/ARP-4754,
    - ED-12B/DO-178B,
    - ED-80/DO-254,
    - ED-14F/DO-160F ;
  - Permettre néanmoins certaines spécificités des aéronefs militaires (temps guerre/temps de paix, mesures d'urgences, largages, etc.) ;
  - Les drones sont soumis généralement au code USAR ou à d'autres règlements particuliers.

Navigabilité des aéronefs militaires et d'Etat (3/3)

- Mise en œuvre de ces recommandations :
  - Prendre en compte les aéronefs mis en service avant la sortie de la règlementation :
    - Délivrer un certificat de type sur la base de l'expérience en service,
    - Appliquer autant que possible la réglementation aux équipements rétro-fittés ou aux évolutions fonctionnelles,
    - Difficulté de dérouler un processus complet dans un ensemble de systèmes hétérogènes et de générations différentes ;
  - Tous les nouveaux aéronefs et tous les nouveaux moteurs sont soumis à la nouvelle réglementation. Pour certains, une certification civile est demandée à l'EASA. Une certification mixte est menée par l'autorité militaire et par l'EASA ;
  - Pas de reconnaissance formelle entre la réglementation civile et la réglementation militaire.

QUESTIONS

Plan de la présentation

Annexe :

évolution du domaine CNS/ATM.

CE 482/2008 : pour les logiciels
Applicable à qui ?

- S'applique aux organisations :
  - Prestataire de Services de Navigation Aérienne rendant des services de circulation aérienne (ATS) et de communication, de navigation ou de surveillance (CNS)
  - Entités assurant la gestion des courants de trafic aérien (ATFM) ou la gestion de l'espace aérien (ASM)

Lorsque l'organisation doit mettre en œuvre un processus d'évaluation et d'atténuation des risques, elle doit définir et mettre en œuvre un « Système d'assurance de la Sécurité des Logiciels » (SASL)

- Deux dates d'application :
  - Pour les logiciels nouveaux : à partir du 1er janvier 2009
  - Pour les modifications de logiciels : à partir du 1er juillet 2010.

CE 482/2008 : pour les logiciels
La démarche et les objectifs

- Des objectifs à atteindre :
  - Validation des exigences
  - Traçabilité des exigences
  - Aucune fonction nuisant à la sécurité
  - Vérification des exigences
  - Gestion de configuration

Les preuves que les objectifs sont atteints doivent être à disposition de l'Autorité Nationale de Surveillance (ANS)

- Objectifs à atteindre avec plus ou moins de confiance :
  - Niveau d'assurance logicielle (SWAL)
  - 4 niveaux minimum
- Obligation de faire du REX
  - Vis-à-vis de l'adéquation du SASL :
    - Vérifier que le niveau du SWAL requis est adéquat
    - Vérifier que les acivités liées à un SWAL donné sont adéquates
  - Vis-à-vis de la détection & correction des problèmes

- La totalité du cycle de vie est pris en compte : de la décision de produire au retrait de service.

CE 482/2008 : pour les logiciels
Difficultés (1/2)

- Un règlement réputé difficilement compréhensible, réservé à des spécialistes :
  - Qui n'a pas bonne presse,
  - Souvent perçu comme une démarche qualité dans le mauvais sens du terme ;
- Beaucoup de logiciels pré-existants, pour lesquels une démarche formalisée d'assurance logicielle n'a pas été menée
  - Démarche rétro-active impossible dans la plupart des cas ;
- Beaucoup de logiciels utilisés sans maîtrise sur le cycle de vie (COTS, COTS adaptés, etc.) ;
- Des logiciels très volumineux.

CE 482/2008 : pour les logiciels
Difficultés (2/2)

- Règlement très peu prescriptif :
  - Ne fixe que des objectifs
  - Pas de norme détaillée imposée
  - La manière d'atteindre ces objectifs est laissée au libre choix des « organisations »

Volonté explicite lors de l'élaboration du règlement basé notamment sur l'ESARR 6

- Règlement qui n'est pas reconnu par toutes les ANS européennes :
  - CAA UK a tenté de s'opposer à la parution d'ESARR 6 puis à celle du règlement CE 482/2008

- Pas de moyen de conformité publié officiellement, il existe deux candidats :
  - L'ED-109/DO-278 : extension de l'ED-12B comprenant des extensions spécifiques à l'ATM mais qui ne couvre pas tout le cycle de vie défini dans le CE 482/2008 et qui ne donne pas de directives pour déterminer le SWAL
  - L'ED-153 « Guidelines for ANS software safety assurance » basé sur les travaux d'Eurocontrol. Cette norme a été reconnue par l'EUROCAE en septembre 2009.