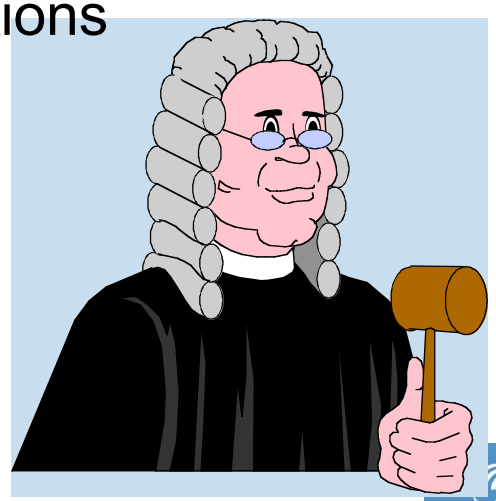
Gérard Ladier
Airbus France
Mars 2003

Le DO 178-B / ED-12B
Logique, historique, contenu, application

Règlement pour les équipements (JAR/FAR 25-1309)

- Les équipements "essentiels" doivent être conçus pour assurer les fonctions attendues
- Les systèmes et les composants, vus seuls ou interconnectés doivent être conçus de telle sorte que l'apparition
  - - de défaillances limitant la sûreté du vol ou de l'atterrissage soit EXTREMEMENT IMPROBABLE
  - - de toute autre nature de défaillance affectant l'intégrité de l'avion ou les actions de l'équipage soit IMPROBABLE
- ...



Comment être conforme au règlement ? Logique.

Un document officiel d'application (AMJ 25.1309/AC 25.1309-1A)

- Impose que la conception des systèmes soit "fail-safe"
- Classifie les conditions de panne selon la sévérité de leurs effets
- Définit les probabilités acceptables des défaillances catastrophiques
- Associe des probabilités acceptables aux différentes classes de conditions de pannes
- Définit les moyens de conformité acceptables pour les différents éléments contributifs.

Comment être conforme au règlement ? Détails

Classification des conditions de panne selon la sévérité de leurs effets

- Catastrophiques : morts multiples, habituellement avec perte de l'avion
- Dangereuses : réduction de la capacité de l'avion ou de l'aptitude de l'équipage à faire face à des conditions opérationnelles défavorables risquant d'entraîner :
  - une réduction important des marges de sécurité ou des capacités fonctionnelles
  - des détresses physiques ou une charge de travail telle qu'on ne pourrait plus compter sur l'équipage pour accomplir ses tâches
  - ou des blessures sérieuses ou des morts concernant un nombre relativement faible d'occupants
- Majeures : réduction de la capacité de l'avion ou de l'aptitude de l'équipage à faire face à des conditions opérationnelles défavorables risquant d'entraîner :
  - une réduction significative des marges de sécurité
  - ou une réduction significative des capacités fonctionnelles
  - ou une augmentation significative de la charge de travail de l'équipage ou des conditions réduisant son efficacité
  - ou un inconfort pour les passagers et équipages, pouvant inclure des blessures
- Mineures : pas de réduction significative de la sûreté de l'avion
- Sans effet sur la sécurité

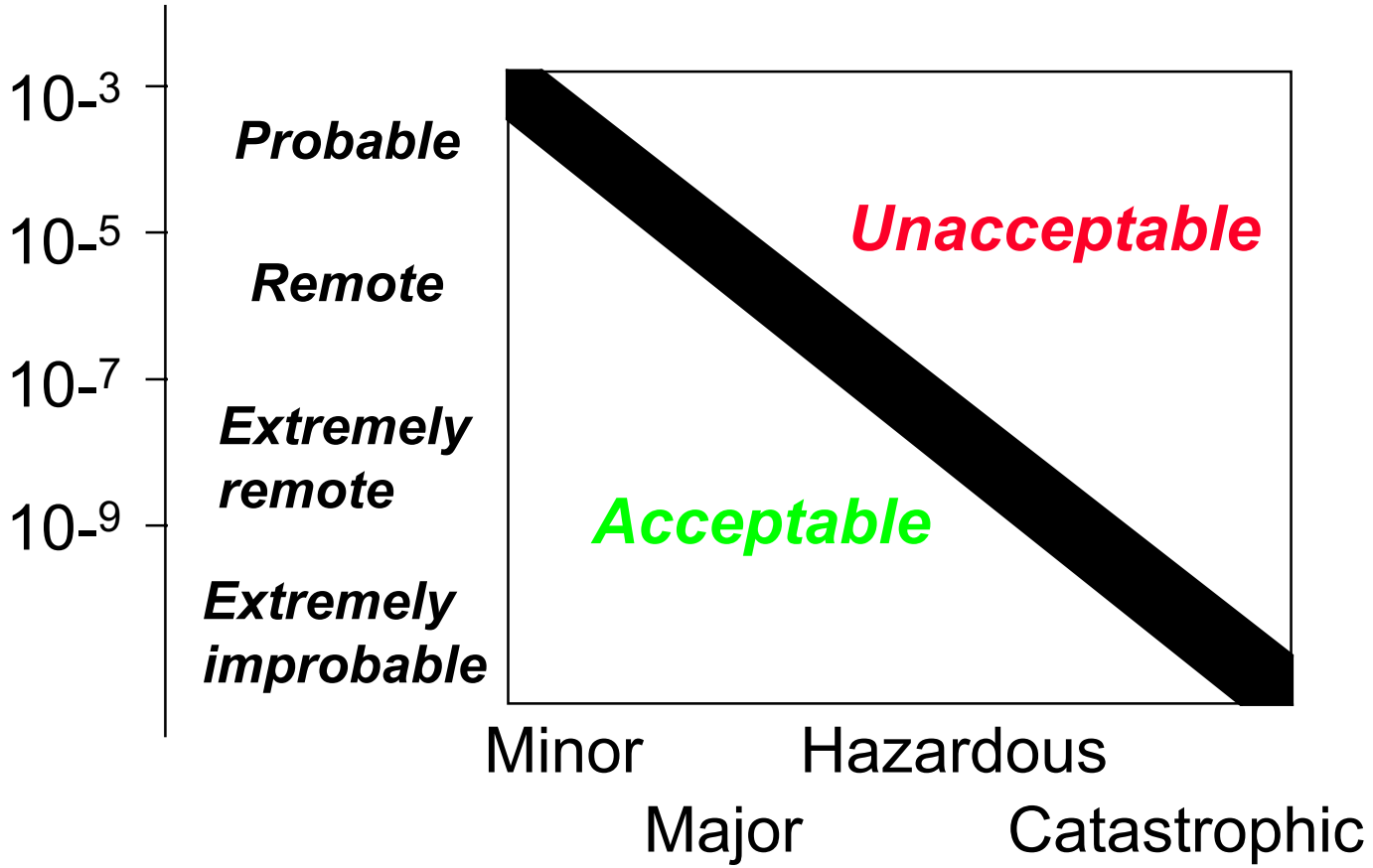
Comment être conforme au règlement ? Détails

Définition des probabilités acceptables des défaillances catastrophiques

- Constat : 1 accident grave pour 10^6 heures de vol
- Constat : 10% sont dus à des défaillances des systèmes avions
- Première conclusion : seuil acceptable d'accidents sérieux imputables aux systèmes : 10^{-7} par heure de vol
- Arbitrairement, on considère qu'une centaine (10^2) de conditions de pannes peuvent être catastrophiques et que chacune a la même probabilité d'occurrence.
- On définit ainsi la probabilité acceptable d'UNE condition de panne catastrophique par heure de vol : 10^{-9}

Comment être conforme au règlement ? Détails

Association des probabilités acceptables aux différentes classes de conditions de pannes



Les moyens de conformité au règlement

Les AMJ 251309 / AC 25.1309-1A présentent des moyens acceptables pour démontrer la conformité aux exigences des JAR/FAR 25.1309 relatives aux équipements. Mais le logiciel est un “être étrange”, et on ne peut le traiter comme le reste :

•It is in general not feasible to assess the number or kinds of software errors, if any, that may remain after the completion of system design, development, and test.

Comme on ne peut pas garantir la sûreté de fonctionnement en se basant sur une évaluation du produit logiciel, on va donc s ’intéresser à son processus de développement

on ne peut pas délivrer de l ’eau propre avec un tuyau sale

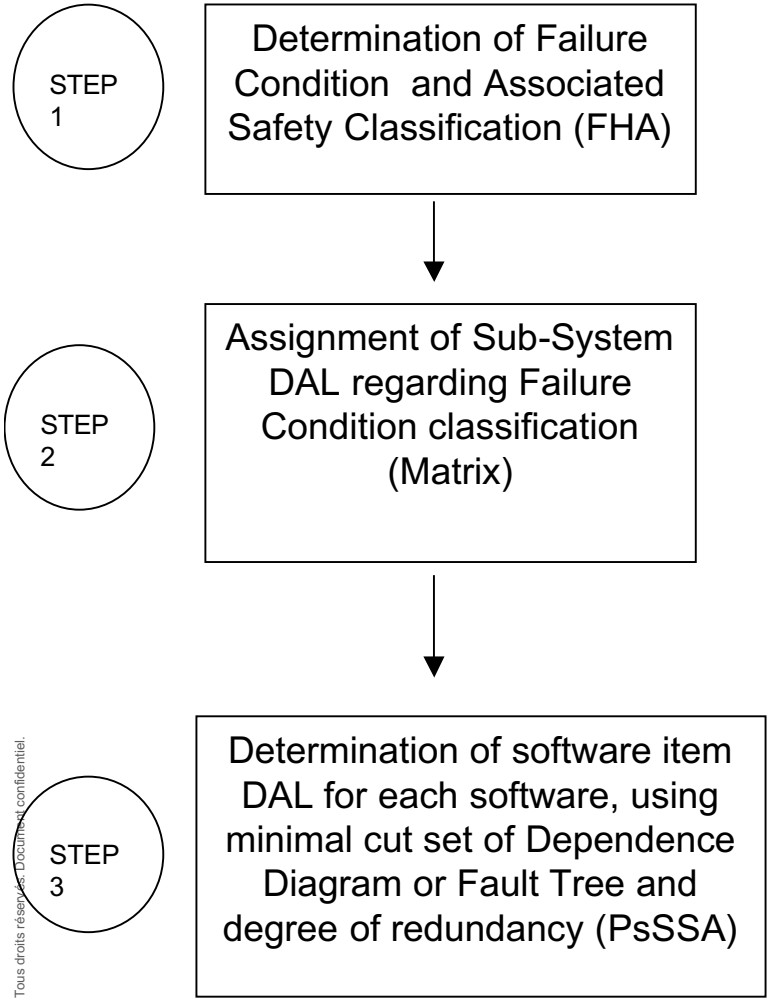
Comment être conforme au règlement ?

Pour détecter et corriger les erreurs de spécification, de conception et de réalisation des systèmes complexes, on s'appuie sur l'Assurance du Développement de ces systèmes.

Actions planifiées et systématiques nécessaires pour fournir un niveau adéquat de confiance et de preuves qu'un produit ou un processus satisfait des exigences données

Le degré d'Assurance exigé est déterminé par la sévérité des effets potentiels des erreurs concernées.

Du règlement à l ’ED-12B : les niveaux

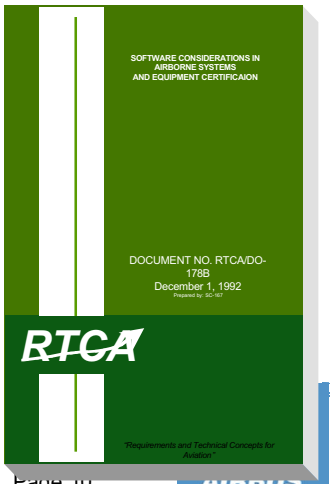


Failure Condition	System DAL (Development Assurance Level)
Catastrophic	A
Hazardous	B
Major	C
Minor	D
No safety effect	E

Une fois le DAL déterminé par analyse de sécurité, on doit respecter les exigences de l ’ED-12B pour ce niveau

L ’ED-12B - Anatomie

- Une section établit le lien avec les aspects "système"
- Plusieurs sections précisent les exigences (objectifs d'Assurance et moyens de les satisfaire) sur chaque processus et sur le cycle de vie
- Une section résume les demandes de données du cycle de vie (~ doc)
- Une section apporte des "considérations complémentaires"
- Une annexe de l ’ED12B définit pour chaque niveau logiciel :
  - les objectifs applicables et les produits demandés par processus (avec renvois sur le reste du document pour les descriptions précises)
  - le degré d'indépendance des activités des processus
  - la catégorie de contrôle pour les données générées par les activités des processus.



L ’ED-12B - Cycles de vie et processus

- Pas de cycle de vie imposé
- Définition des processus séparés qui seront combinés pour un projet donné pour décrire son cycle de vie :
  - Processus de planification (organisation/plans plutôt que planning)
  - Processus de développement (spécification, conception, codage, intégration)
  - Processus intégraux (vérification, gestion de configuration, assurance qualité, coordination pour la certification).

L ’ED-12B - Les processus

- Définition pour chaque processus :
  - des objectifs d'Assurance (ex : détecter les erreurs introduites au cours du développement)
  - des moyens de les satisfaire (ex : combinaison de revues, d'analyse, et de tests)
  - des données d'entrées du processus (ex : spécifications, code source, plan de vérification)
  - des activités du processus (ex : revues et analyses diverses, tests divers fondés sur les exigences)
  - des produits du processus (ex : jeux, procédures et résultats de vérification)
  - des critères de transition, qui doivent être satisfaits pour l'engager
- En général, pas de définition précise des méthodes ou des moyens à utiliser (par exemple, il n'impose pas de faire des tests unitaires).

L ’ED-12B - La vérification

- La section la plus importante de l ’ED-12B
  - en volume : 13 pages de description (5 pages en moyenne pour les autres)
  - en charges de travail (et de justification) induites....

- Principes de base :
  - processus transverse => s'applique à tous les processus de développement
  - combinaison de revues, d'analyses et de test pour détecter et rendre compte des erreurs introduites au cours du développement
  - test fonctionnel (fondé sur les exigences)
  - PAS DE TEST FONDE SUR LA STRUCTURE DU CODE
  - analyses de couverture "fonctionnelle" et "structurelle".

L ’ED-12B - coordination pour la certification

- Objectif :
  garantir une bonne communication/compréhension entre le postulant et l'autorité de certification
- Moyens :
  - Le Plan des Aspects Logiciels de la Certification, communiqué le plus tôt possible aux autorités
  - Des revues, menées par les spécialistes "logiciel" des autorités de certification à leur discrétion.
  - Le Résumé des Travaux Réalisés et le Répertoire de la Configuration du logiciel.

L ’ED-12B - Section 12 - Qualification des outils

- Nécessaire quand des processus requis par le reste de l ’ED-12B sont éliminés, réduits, ou automatisés par l'utilisation d'un outil (déterministe) dont les sorties ne sont pas vérifiées

- 2 catégories d ’outils, définies en fonction du risque d ’erreur :
  - outils de développement (ex : générateur de code)

    Exigences en gros équivalentes à celles du niveau du logiciel généré

  - outils de vérification (ex : émulateurs, simulateurs)

    Exigences réduites (3 lignes contre 53), limitées à la validation de l'outil, néanmoins sujettes à beaucoup d'interprétations très différentes suivant les interlocuteurs des autorités de certification.

ED-12B -Variations par niveaux

- Niveaux A et B très proches
  - autant d'objectifs chacun (à un près concernant la couverture structurelle)
  - ils se différencient essentiellement par le degré d'indépendance requis dans l'atteinte des objectifs (40 % avec indépendance pour le A, 20% pour le B)
- Niveau C ~ 85 % des niveaux A/B (nb d'objectifs)
  - La variation est surtout sensible sur le processus de conception, sur l'exigence de couverture structurelle des tests, et sur l ’indépendance
- Niveau D ~ 50 % du niveau C (nb d'objectifs)
  - Quasiment plus aucune exigence sur la spécification, la conception, le codage, l'intégration, la vérification
- Niveau E : Aucune exigence
  - "une fois que l'autorité de certification a confirmé qu'un logiciel est de niveau E"

Questions sur l ’ED-12B et son application

L ’application de l’ED 12-B coûte trop cher ?

- 1997, SSAC : "*make recommendations to the FAA to reduce the cost and time associated with software aspects of certification for both airborne and ground-based software while maintaining or improving safety*”.
- Enquête menée auprès de l ’industrie US. 240 questions posées, 300 retours. Questions posées sur l ’ED-12B :

$ $ Independence does not add value

$ $ MC/DC does not add value

$ $ Quality assurance does not add value

$ $ Traceability does not add value

$ $ Unreasonable requests for documentation

$ $ Tool qualification does not add value

$ $ Another specific question was also asked on the connection between DO-178B/ED-12B and safety.

Site SSAC : http:// shemesh.larc.nasa.gov/ssac/

L ’application de l’ED 12-B coûte trop cher ?

- Mais les retours ne sont pas ceux escomptés :
  - Indépendance : 82 % la juge extrêmement ou assez valable
  - Traçabilité : jugée efficace, même si c ’est coûteux
  - Assurance qualité : entre 57% et 79% (suivant questions) la considère extrêmement ou assez valable
  - Qualification des outils : tous ont trouvé des erreurs pendant la qualification, qui ne coûte pas si cher que ça
  - L ’analyse de couverture structurelle MC/DC : 12% des industriels n ’ont jamais trouvé d ’erreur avec cette technique, certes très coûteuse.
  - La documentation fut le seul point pour lequel le présupposé est validé par l ’étude, mais une enquête approfondie a montré une incompréhension des exigences réelles dans ce domaine.

Et si on certifiait le logiciel seul ?

- 1996. Une partie de la FAA (>free flight) veut révolutionner la certification : *currently, computer hardware and software has to be certified as a "system" for every installation. We're suggesting that standards be developed so that software can be certified as a discrete appliance, irrespective of the operating system or hardware platform.(…)*

- Cette approche « plug & play » a fait long feu (on ne certifie pas un logiciel, mais un système complet).

- Mais le concept d ’avionique modulaire intégrée de l ’A380 et sa « qualification incrémentale » peut constituer un (petit) pas dans cette direction.

Rendez-vous en 2006 !

Utiliser des COTS en avionique ?

L 'ED-12B et les COTS :

•Spécificité COTS ?

2.4/f « Logiciels du commerce sur étagère : Les logiciels de ce type inclus dans les systèmes ou équipements de bord doivent satisfaire les objectifs de ce document »

• Comme tout le reste ...

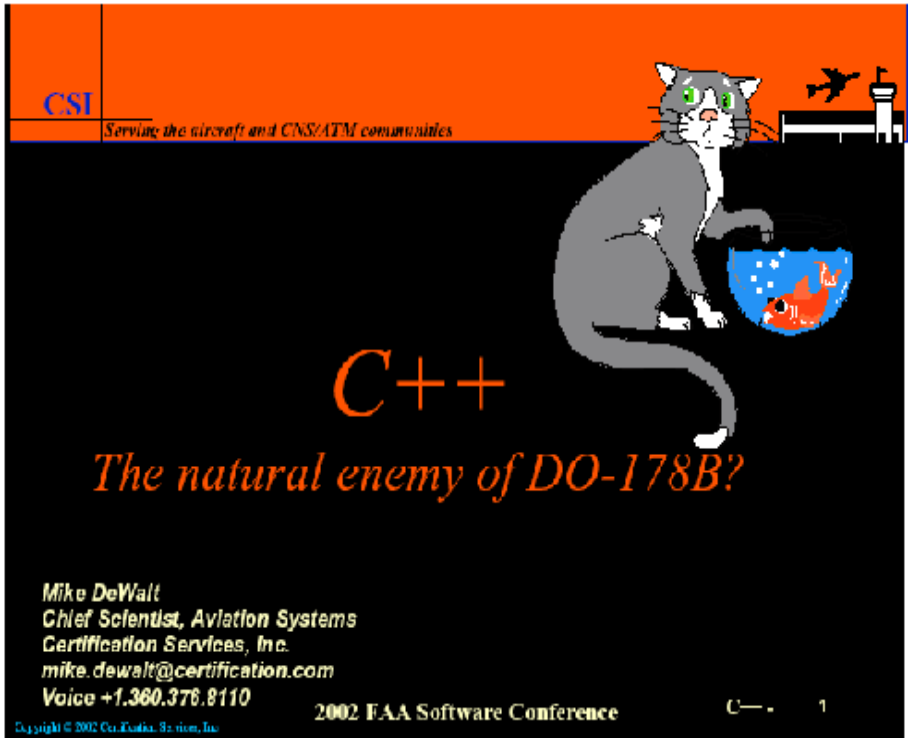
2.4/g « S 'il existe des insuffisances dans les données du cycle de vie des logiciels du commerce sur étagère, il est nécessaire de compléter ces données de manière à satisfaire les objectifs de ce document … »

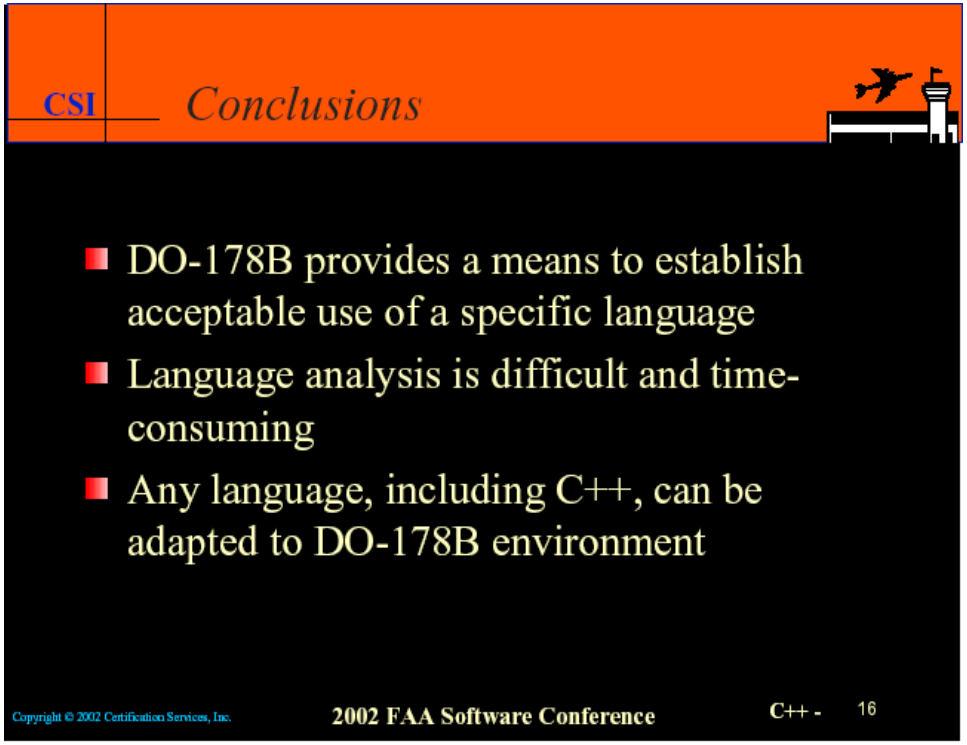
- Contradiction entre besoin industriel d 'utilisation de COTS et approche processus (vs. approche produit) de l 'ED-12B.
- Peut se révéler contre productif du point de vue de la sûreté de fonctionnement ...

Peut-on utiliser l ’approche objet ?

- Le sujet est encore débattu, mais des applications existent déjà.
- Mike Dewalt a bien résumé la situation

(http://av-info.faa.gov/software/conferences.htm) :





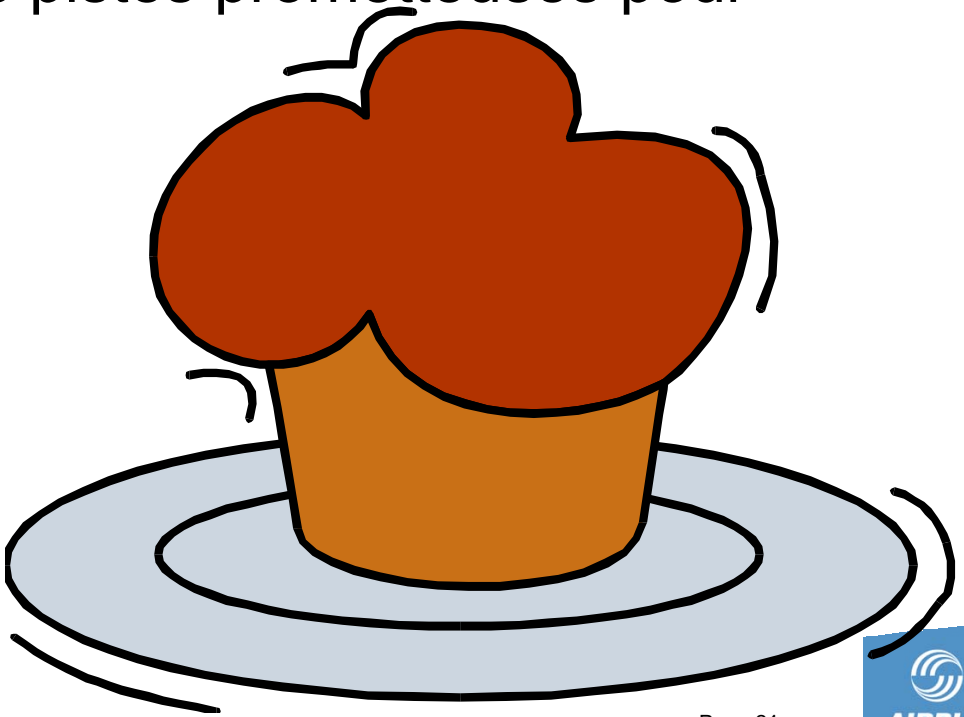
Remplacer le test par la preuve ?

- L'ED-12B est prescriptif en terme de moyen de vérification
- La preuve de propriété est séduisante
  - exhaustivité
  - analyse du source (binaire possible à terme)
  - effort supplémentaire de conception
  - économie :
    - pas de phase coûteuse d 'identification des cas de test
    - pas de moyens matériels spécifiques
    - automatisation poussée voire totale
- Une première application industrielle est en cours sur l 'A380
- Si généralisation, la contradiction avec l 'ED-12B devra être levée (il faut revenir à l 'objectif de la vérification, alors que l 'ED-12B actuel raisonne sur cet aspect en terme de moyen)

La suite ?

- The proof of the pudding is the eating : l ’approche assurance du développement fonctionne.
- Mais ça reste une approche par défaut : « je ne sais pas assurer la qualité de mon produit, je vais donc assurer la qualité de son processus de développement »
- On commence à entrevoir des pistes prometteuses pour (re)venir à une approche « assurance produit »

A développer pour rendre le pudding plus digeste !



Introduction