Jama software®

LIVRE BLANC

Bonnes Pratiques DO-178C à Destination des Ingénieurs et des Managers

By Vance Hilderman

Bonnes Pratiques DO-178C : Introduction

La pratique nous concerne tous à un moment ou un autre. Qu'il s'agisse du piano, des mathématiques, du golf ou du pilotage, la pratique implique généralement une bonne dose de coaching, un peu d'autocritique et pas mal de répétition. Cependant, le développement en avionique laisse peu de place à la pratique, car chaque détail compte. Et comme les délais, les budgets et la sécurité sont tous en jeu, chaque erreur peut coûter cher. Comment alors réconcilier « pratique » et développement en avionique ? La meilleure solution consiste à comprendre l'ampleur du développement mondial et de rassembler les meilleures connaissances et méthodes dans le domaine. Bienvenue dans le guide des bonnes pratiques DO-178C.

En vol, il est nécessaire de faire des compromis entre la charge utile, la portée, la vitesse et les coûts. La large variété d'avions disponibles sur le marché aujourd'hui est la preuve que de nombreuses personnes priorisent ces compromis différemment. Mais les différences dans les pratiques de développement de logiciels d'avionique sont bien plus limitées. Tout le monde cherche à minimiser les aspects suivants :

- Coût
- Délais
- Risques
- Anomalies
- Difficulté de réutilisation
- Obstacles à la certification

Les pages qui suivent présentent les bonnes pratiques du standard DO-178C permettant de minimiser ces six aspects importants dans votre développement.

Bonnes Pratiques DC-178C : Préambule

Certaines bonnes pratiques pour le développement de logiciels d'avionique sont évidentes. Comme en matière de santé, chacun sait qu'une alimentation équilibrée, l'exercice physique, le sommeil et la réduction du stress sont de « bonnes pratiques ». Pour les logiciels, les bonnes pratiques évidentes incluent la prévention des anomalies, le recours à des développeurs expérimentés, les tests automatisés et la limitation des changements. Cet article n'aborde pas ces évidences car nous considérons qu'un lecteur qui arrive sur cette page possède déjà certaines connaissances. Les bonnes pratiques DO-178C identifiées ici sont plus subtiles et leur application plus rare.

Le schéma suivant présente le top 10 des bonnes pratiques DO-178C « pas toujours évidentes »

Top 10 des bonnes pratiques « méconnues » pour DO-178C

01
EBN Plus Détaillées

Les exigences sont la base d'une ingénierie de qualité. Les exigences détaillées sont la base d'une ingénierie remarquable.

Des chercheurs ont prouvé depuis longtemps que la plupart des défauts logiciels sont dus à des exigences faibles. Dans son livre *Mythical Man-Month*, Frederick Brooks estime que les suppositions sont l'une des principales causes des défauts logiciels. Le standard DO-178C a été intentionnellement renforcé par rapport à son prédécesseur, DO-178B, afin de garantir des exigences acceptables. Pour y parvenir, 178C exige qu'il soit possible de retracer les analyses de couverture structurelle jusqu'aux aux tests basés sur les exigences (TBE). Rappelez-vous : DO-178C ne fournit pas de standards d'exigences stricts, mais il en faut pour les niveaux DAL (Development Assurance Level) A, B et C. Ces standards doivent définir la portée et les détails associés aux exigences de haut niveau (EHN) et aux exigences de bas niveau (EBN). Dans l'idéal, le standard des exigences comprend des exemples d'EHN comparées à des EBN. Les checklists pour la revue des exigences doivent également contenir de nombreux critères permettant d'évaluer le niveau de détail des EBN.

02
Définition d'un Scénario de Test Parallèle

Si un testeur ne comprend pas avec certitude le sens d'une exigence de logiciel, comment le développeur le pourrait-il ?

DO-178C ne se préoccupe pas des coûts et des délais : le développeur est libre d'être en retard et de dépasser son budget. Bien que les critères de transition doivent être explicitement définis pour toutes les phases de développement des logiciels, il est courant que les entreprises définissent leurs scénarios de test après l'écriture du logiciel. Cependant, les grandes entreprises définissent les scénarios de test avant même que le code ne soit écrit. Pourquoi ? Parce qu'il vaut mieux

prévenir les erreurs que les détecter lors des tests. Si un testeur ne comprend pas avec certitude le sens d'une exigence de logiciel, comment le développeur le pourrait-il ? Les entreprises averties vérifient les exigences indépendamment en demandant au testeur de définir des scénarios de test dans le cadre de la revue des exigences, avant que le code ne soit écrit. Les ambiguïtés ou les lacunes des exigences sont corrigées plus tôt, ce qui réduit le nombre d'anomalies logicielles et accélère les tests.

03
Mise en Œuvre des Standards de Test

Standard d'exigences. Standard de conception. Standard de codage. Standard de test....

Attendez, il n'y a pas de standard de test ?

DO-178C demande explicitement des standards pour les niveaux DAL A, B et C. Quels standards ? Exigences, conception et code. Pourquoi DO-178C n'exige-t-il pas un standard de vérification ou de test ? A priori, il y a moins de variations dans les tests que dans les phases précédentes du cycle de vie, qui sont effectivement plus variables d'une entreprise à l'autre et d'un projet à l'autre. Personne n'a jamais accusé DO-178C de demander trop peu de documents. À cause du fonctionnement en cascade traditionnel (hérité du DO-178A il y a vingt ans), de nombreux documents sont déjà nécessaires. Cependant, les entreprises efficaces reconnaissent le coût et la subjectivité de la vérification et admettent qu'il vaut mieux la gérer avec un standard de test logiciel. Puisqu'il n'est pas officiellement requis, il n'a pas besoin d'approbation ou de soumission. Qu'est-ce qu'un tel standard de test hypothétique est censé couvrir ? Au moins les éléments suivants :

- Description des TBE pour obtenir la couverture structurelle
- Détails sur la granularité de la traçabilité pour les procédures de test et les scénarios de test
- Explications sur l'évaluation de la couverture structurelle par niveau DAL applicable
- Définition des tests de robustesse, appliqués aux exigences et au code (selon les niveaux DAL applicables)
- Pour le niveau DAL A, explications de la MC/DC applicable et corrélation source/binaire
- Couplage des pratiques d'analyse, y compris le rôle des revues de code et de conception
- Critères de test basés sur les performances
- Exemples d'exigences et de code, avec les scénarios de test associés recommandés

04
Modèles de Canevas de Modélisation

La modélisation logicielle finira par disparaître... à condition que la fonctionnalité, la complexité et la taille des logiciels diminuent toutes de 90 %.

Il y a peu de paris sans risque dans la vie. Cependant, l'auteur affirme qu'on peut gager sans risque que la fonctionnalité, la complexité et la taille des logiciels continueront à augmenter. Tout comme l'exercice physique aide à compenser une alimentation riche en matières grasses, la modélisation logicielle permet de mieux gérer les logiciels de demain. Cependant, les modèles et les techniques de modélisation peuvent grandement varier. Une grande variation au sein d'un projet annihile la plupart des avantages de la modélisation, notamment en ce qui concerne la vérification et la réutilisation. Une bonne pratique ? Utiliser des canevas de modélisation et les définir dans le standard de conception du projet. Les canevas de modélisation doublés d'une vérification et d'une réutilisation cohérentes permettent de gérer la complexité des logiciels.

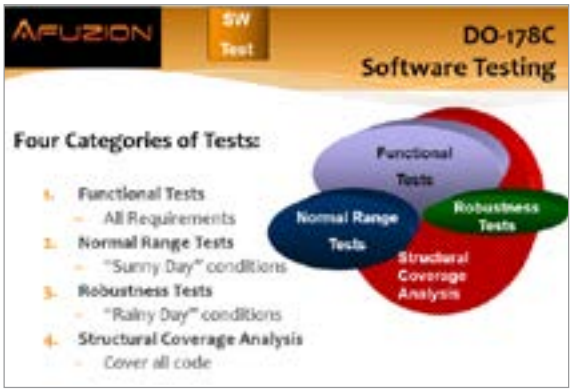
05
Des Réviseurs Moins Nombreux Mais plus Compétents

Un excellent réviseur vaut mieux que plusieurs bons réviseurs. Si la quantité faisait toujours la qualité, les avions auraient 10 moteurs....

L'auteur n'a jamais vu un avion à 10 moteurs, mais il a vu beaucoup d'équipes d'évaluation par des pairs comptant 10 ingénieurs. Pourquoi tant de réviseurs ? Était-ce de l'optimisme ? Du pragmatisme ? Ou peut-être simplement de la naïveté ? Il n'est pas rare de penser que la quantité peut faire la qualité... Mais dans le cas des revues de logiciels, la solution est de n'avoir qu'un seul excellent réviseur. Un réviseur d'excellent niveau est plus rentable, plus productif et, doté des compétences appropriées, meilleur.

06
Régression Automatisée et Intégration Continue

Les tests de logiciels ne devraient pas être considérés comme un luxe, mais comme une nécessité. DO-178C exige une variété de tests nécessaires, avec un niveau de rigueur indexé sur la criticité. Les types de tests de base sont présentés ci-dessous :



DO-178C exige une analyse de régression dans laquelle les mises à jour logicielles sont évaluées pour déterminer si elles risquent d'impacter le logiciel déjà testé, et de nouveaux tests sont effectués en cas de résultat positif. On consacre plus de temps aux tests qu'au développement. C'est vrai pendant le cycle de vie du projet, mais c'est encore plus vrai pendant le cycle de vie du produit. Beaucoup considèrent que les tests de logiciels constituent le plus grand poste de dépense dans le cadre de

DO-178C. Investir du temps en amont pour élaborer un cadre d'automatisation des tests peut s'avérer être le plus grand vecteur d'économies. Et l'intégration continue, qui teste automatiquement et continuellement les changements, est le meilleur moyen d'atteindre les objectifs de régression. Pourquoi ? En retestant continuellement tous les logiciels, l'analyse de régression est grandement simplifiée : il suffit de répéter tous les tests en appuyant sur un bouton.

07
Vérificateur Automatique de Règles de Conception

Dans des conditions favorables, les performances de l'être humain sont satisfaisantes lorsqu'il vérifie les règles de conception d'un logiciel. Mais dans le monde de la sécurité, les conditions ne sont pas toujours favorables.

Le monde des logiciels de sécurité critiques abonde en outils et techniques d'analyse de code statique, d'automatisation des tests, de couverture structurelle et de conception basée sur des modèles. Cependant, si une imperfection peut être vue comme un défaut, alors les activités citées ci-dessus ratent tout un pan des défaillances de conception. Rappelez-vous : les suppositions sont l'une des principales causes d'anomalies logicielles, d'où la nécessité d'avoir des exigences détaillées, de la traçabilité, des standards de codage, etc. Cependant, chaque personne aura ses propres suppositions quant à la conception du logiciel et aux interfaces internes. Ces différentes suppositions mènent à des composants logiciels mal coordonnés et ces imperfections peuvent masquer des défauts. La solution ? Des vérificateurs automatiques de règles de conception qui aident à garantir une exécution et des interfaces cohérentes et déterministes. Avec les modèles de canevas de modélisation évoqués au point 4, ils forment une combinaison puissante.

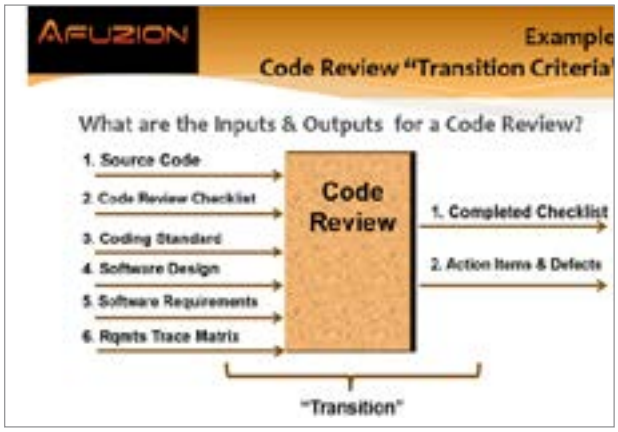
08
Tests de Performance Avancés

Étrangement, DO-178C fournit très peu de directives quant aux tests de performances. C'est l'origine d'un écueil très commun : des tests de performances minimaux. Pourtant, les tests de performance approfondis sont le signe d'un logiciel de qualité et le seul moyen de détecter certaines anomalies qui, autrement, resteront inconnues jusqu'à des défaillances en vol potentiellement catastrophiques. Bien souvent, la correction des anomalies de logiciel liées aux performances nécessite des modifications d'architecture majeures, coûteuses et chronophages. Comment faire autrement ? En réalisant des tests de performances avancés permettant de :

- Définir les pires cas de charges avec les temps d'exécution au pire cas (WCET)
- Utiliser un taux de changement maximal continu pour les entrées dans toutes les interfaces.
- Vérifier une à une les exigences de performances distinctes exigées par DO-178C.

- Prendre en compte les opérations en mode dégradé lorsque les entrées principales ne sont pas disponibles, ce qui nécessite l'utilisation d'entrées secondaires qui demandent plus de puissance de calcul.
- Utiliser les données des paramètres pire-cas, chaque paramètre étant délibérément choisi en fonction de son impact sur le WCET.

09
Audits de Traçabilité Parallèle et de Transition



Alors que l'athlète amateur se concentre sur le résultat, le professionnel se concentre sur l'optimisation de la technique, puisque le résultat en dépend. Les développeurs amateurs et professionnels savent que la réduction des anomalies est un objectif, mais le professionnel sait que la technique est importante. En avionique, cela se traduit par les critères DO-178C de traçabilité et de transition. Là où les amateurs évaluent la traçabilité et les critères de transition à la fin, avec SOI-4, les professionnels déploient une AQL active et des outils pour surveiller continuellement la traçabilité bidirectionnelle. Insistez sur les vérifications des critères de transition dès le début, comblez les lacunes du processus et enregistrez les résultats de la vérification. Souvenez-vous que chaque type de revue des artefacts constitue une transition : les ingénieurs doivent respecter les critères de transition définis et l'AQ doit procéder à une vérification pour évaluer la conformité du processus. Un exemple de transition de revue de code est présenté ci-dessous. Assurez-vous que toutes les entrées et sorties sont parfaitement utilisées, présentes dans la gestion de configuration et référencées dans les résultats.

10
Ateliers de Formation Technique

Quel que soit le secteur d'activité, les ingrédients pour être « le meilleur » sont un savant mélange de formation, de coaching, et de pratique. Les groupes d'avionique qui suivent les bonnes pratiques intègrent les deux premiers ingrédients grâce à la formation. Qu'elle soit dispensée en interne ou en externe, une formation technique améliore les chances d'une certification DO-178C réussie. Quelle formation choisir ? Il vaut mieux se concentrer sur les aspects très rentables, parmi lesquels l'amélioration de la productivité et de l'homogénéité des processus critiques suivants :

- Rédaction des exigences (met l'accent sur la granularité moyenne pour assurer l'homogénéité)
- Tests de logiciels (met l'accent sur l'exhaustivité et des scénarios complets et réalistes faisant usage des interfaces inter-domaines)
- Revues (met l'accent sur le standard, les détails, la robustesse, les modifications et l'identification des anomalies importantes)
- Vérification et détection/correction de véritables anomalies (met l'accent sur le processus des critères de transition)

Pour plus d'informations sur la formation DO-178C avancée, rendez-vous sur :

afuzion.com/training

Pour plus d'informations sur l'analyse des écarts DO-178C, rendez-vous sur :

afuzion.com/gap-analysis

Qu'est-ce que AFuzion ? Présentation en une minute :

www.youtube.com/watch?v=RMzLRzcahJE

Pour plus de détails sur DO-178 et DO-254, consultez le livre *Avionics Certification: A Complete Guide To DO-178 & DO-254*, disponible dans les grandes librairies comme Amazon.com. (L'auteur de cet article en est le principal auteur.) En outre, le livre *The Avionics Development Ecosystem* de Vance Hilderman aborde le développement en avionique dans son ensemble, de la sécurité aux systèmes en passant par tous les aspects essentiels de la réglementation et de la conception pour le développement moderne en avionique. Rendez-vous sur le site de AFuzion, www.afuzion.com, pour accéder à des modules de formation avancée adressés aux débutants comme aux experts en DO-178C.

À PROPOS DE VANCE HILDERMAN

Vance Hilderman est le fondateur de deux des plus grandes sociétés au monde de services de développement en avionique. Il a également créé la première formation DO-178 au monde et formé plus de 8 000 ingénieurs dans 45 pays à DO-178, DO-254, DO-278 et DO-200A. Enfin, c'est l'auteur principal du premier livre au monde sur DO-178 et DO-254.

À PROPOS DE JAMA SOFTWARE

Jama Software fournit la plateforme leader pour la gestion des exigences, des risques et des tests. Les équipes en charge de la production de produits, systèmes et logiciels complexes peuvent s'appuyer sur Jama Connect et sur des services pour raccourcir les temps de cycle (par secteur industriel), améliorer la qualité, réduire les corrections et minimiser les efforts tout en garantissant la conformité du produit. Jama compte une clientèle toujours plus nombreuse, réunissant plus de 600 organisations à la pointe des évolutions en matière de développement dans les secteurs de l'automobile, de l'appareillage médical, des services financiers, de la fabrication industrielle et de l'aérospatiale.