Jama software®

LIVRE BLANC

# Exigences en Aéronautique Pour les Solutions Matérielles/ Logicielles Embarquées et au Sol

*Par Vance Hilderman, AFuzion*

Les exigences adéquates constituent la base des produits de haute qualité. Dans l'aéronautique, elles sont primordiales pour tous les aspects d'un produit : matériel, logiciel, système et sécurité. Mais comment établir de bonnes exigences ? Que doit contenir un standard d'exigences en aéronautique ? À quoi ressemblent des exigences faibles, satisfaisantes, bonnes et - pour finir - excellentes ? Existe-t-il des différences entre les exigences de l'embarqué et du sol, ou entre les exigences de logiciel et de matériel ? La pérennité du secteur aéronautique nécessite que nous répondions à ces questions.

Nous vous proposons d'abord de répondre au questionnaire suivant sur les exigences. Connaissez-vous les réponses ? Si vous développez des logiciels pour l'aéronautique, il est impératif que vous connaissiez les réponses à ces questions. Les pages suivantes développent ces réponses et abordent également d'autres aspects.

## AFuzion : un Questionnaire sur les Exigences Essentielles de Sécurité

1. V/F : Dans la plupart des projets d'avionique, la majorité des exigences concernent la sécurité.
2. V/F : En avionique, l'élaboration des exigences doit se faire en cascade.
3. V/F : La meilleure façon d'évaluer les exigences essentielles de sécurité est de procéder à des essais.
4. V/F : Les standards DO-178C et ARP4754A fournissent des conseils clairs pour l'élaboration et l'évaluation des exigences.
5. V/F : La plupart des défauts d'avionique sont dus à des bugs et à des défauts de fabrication.
6. V/F : Dans le contexte du développement basé sur des modèles, les exigences système et logiciel doivent être textuelles et externes au modèle.

Il serait tentant de demander aux autorités de certification quelles exigences sont les plus importantes entre celles des systèmes, des matériels, des logiciels embarqués et des systèmes au sol. Cependant, cela pourrait amener à penser, à tort, qu'il faudrait les prioriser les unes par rapport aux autres. Comme l'ont conclu de nombreux experts en développement de systèmes critiques, les exigences sont la base du développement en aéronautique. Les experts en sécurité de renommée mondiale affirment systématiquement que la cause première des défauts liés à la sécurité est la faiblesse des exigences. La faiblesse des exigences en question provient d'un développement basé sur des suppositions, dans un contexte où différents ingénieurs font des suppositions différentes. Si les suppositions sont différentes, il est logique qu'au moins l'une d'elles, sinon toutes, soit fausse.

Cependant, les directives pour l'aéronautique sur lesquelles les autorités de certification aéronautique s'appuient sont vagues en ce qui concerne les méthodologies pour élaborer des exigences optimales. Bien que beaucoup croient à tort qu'il s'agit d'une faiblesse de ces directives, la vérité est plus subtile :

1. Les systèmes aéronautiques diffèrent grandement par leur fonctionnalité, leur criticité et les méthodologies de développement choisies. Par conséquent, un seul guide de rédaction des exigences n'est pas suffisant.
2. On s'appuie plutôt sur le « standard des exigences » détaillé fourni avec chaque projet aéronautique. Il décrit en détail l'approche spécifique du projet quant à l'élaboration des exigences et de leurs critères d'évaluation.

## Vérification et Validation

Imaginons une conversation entre un ingénieur en aéronautique « typique » et un non-ingénieur.

**Non-ingénieur :** « Qu'avez-vous fait aujourd'hui ? »

**Ingénieur :** « J'ai fait de la V&V. »

**Non-ingénieur :** « Qu'est-ce que c'est, la V&V ? »

**Ingénieur :** « Vérification et validation. À moins que ce ne soit validation et vérification. »

**Non-ingénieur :** « Est-ce que vous avez procédé à une validation ou à une vérification ? »

**Ingénieur :** « Oui, j'ai fait de la V&V. »

**Non-ingénieur :** « Mais est-ce que vous avez procédé à une validation ou à une vérification ? »

**Ingénieur :** « Personne ne connaît la différence entre les deux. C'est pour ça que ça s'appelle de la V&V ! »

### En Réalité, la V&V, c'est Facile.

**Vérification :** la mise en œuvre répond-elle aux exigences ?

**Validation :** les exigences sont-elles correctes ?

À présent, demandez aux autorités de certification ce qui est le plus important entre la vérification et la validation. Encore une fois, la réponse la plus sûre est : « Les deux. » La vérification ne doit pas être moins importante que la validation et inversement. Cependant, demandez à un ingénieur en aéronautique chevronné ce qui est le plus important. La seule bonne réponse devrait être : « La validation, parce que si les exigences ne sont

pas bonnes, peu importe que vous les ayez bien vérifiées ! »

C'est exactement ça. La validation des exigences permet de garantir qu'elles sont correctes et complètes. Pour les logiciels d'aéronautique, la validation est réalisée à l'aide du matériel au niveau système. Ainsi, les exigences de logiciel sont techniquement validées via une revue. En revanche, pour ce qui est des exigences de matériel et de système, la validation comprend des revues, des simulations, de la modélisation, des analyses et toute autre combinaison des techniques requises pour garantir la justesse et l'exhaustivité.

À l'heure où la complexité des systèmes aéronautiques augmente, un seul niveau d'exigences est insuffisant. Peut-être qu'à ses débuts, l'aéronautique pouvait se contenter d'un seul niveau d'exigences, mais la complexité croissante et les équipes d'ingénieurs plus grandes augmentent le risque de suppositions erronées. Par conséquent, les systèmes aéronautiques ont de multiples niveaux d'exigences, parmi lesquels :


Niveaux types d'exigences en aéronautique

Chacun des domaines d'exigences ci-dessus présente probablement une granularité croissante, dans l'ordre indiqué. Au fil du processus, des exigences de sécurité supplémentaires peuvent être décomposées ou dérivées, afin de clarifier certains aspects nécessaires du système, du matériel et du logiciel. Lorsque les systèmes sont particulièrement complexes, l'un des domaines d'exigences ci-dessus peut être subdivisé en deux niveaux d'exigences ou plus. Le résultat final est caractérisé par plusieurs niveaux qui offrent une plus grande qualité grâce à une meilleure compréhension des liens entre les exigences et à la capacité de mieux les valider et les vérifier. L'élaboration des exigences en aéronautique implique des décompositions de plus en plus détaillées et des revues des exigences à chaque niveau de raffinement. Pour les niveaux d'assurance plus élevés associés à des effets de défaillance dangereux ou catastrophiques, il faut prouver que la V&V des exigences est indépendante, c'est-à-dire qu'elle est effectuée par une tierce personne suivant un processus indépendant du concepteur des exigences.

Dans le cas d'un logiciel, il n'est pas rare que la complexité ou la taille du logiciel soit si grande que chacun ne comprend qu'une infime partie de la logique. C'est pourquoi l'avionique embarquée (DO-178C) et les systèmes au sol de communication, de navigation et de gestion du trafic aérien (CNS/ATM, DO-278A) nécessitent par défaut deux niveaux d'exigences : les exigences de haut niveau (EHN) et les exigences de bas niveau (EBN).

Les exigences système doivent comprendre l'ensemble des fonctionnalités au niveau du système (boîte noire), y compris les exigences de sécurité. Les exigences système sont ensuite décomposées et attribuées au matériel, au logiciel, ou aux deux. Les EHN de logiciel précisent ensuite ce que le logiciel fait au niveau de l'interface matérielle ou logicielle. Les EHN ne doivent pas présenter de détails au niveau des fonctionnalités ou des modules du logiciel car cela est spécifié dans les EBN. La raison pour laquelle deux niveaux d'exigences de logiciel existent (les EHN et les EBN) est fondamentale : les fonctionnalités logicielles simples peuvent être intégralement décrites avec un seul niveau d'exigences, mais les logiciels d'aéronautique sont de plus en plus complexes. Ainsi, l'explicitation, la mise en œuvre et la vérification des exigences sont plus fiables lorsque la spécification se fait sur deux niveaux de raffinement ou plus.

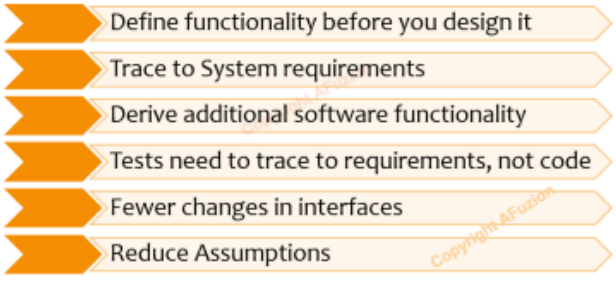
Dans les versions antérieures des directives pour l'aéronautique, comme DO-278 et DO-178B, les objectifs officiels associés aux EHN et aux EBN étaient particulièrement vagues. Il n'y avait pas d'instruction officielle de revenir en arrière pour améliorer les exigences. DO-178C et DO278A ont changé les choses en exigeant que les EBN soient très détaillées (allant jusqu'aux branches logiques) et en forçant l'amélioration des exigences (généralement par la clarification des EBN) lorsque l'analyse de couverture structurelle indique des structures de code non couvertes en raison d'EBN faibles. Par conséquent, les systèmes hérités, en particulier les systèmes CNS/ATM au sol, contiennent généralement des EBN plutôt faibles.

Les directives pour l'aéronautique ne donnent pas de méthode pour la rédaction des exigences. Elles ne définissent pas non plus de frontière distincte entre les EHN et les EBN, ou entre les EBN et la conception. C'est en fait à chaque projet qu'il incombe de fournir une « méthode » vérifiable ainsi que le standard qui lui est propre et grâce auquel les exigences seront évaluées.

## Exigences de Haut Niveau

Le développement d'EHN suit la définition des exigences du système mais précède le développement d'EBN. Les EHN doivent être officiellement revues (voir ci-dessous) avant le développement des EBN associées.

Le graphique suivant met en avant les principales raisons pour lesquelles les EHN sont nécessaires pour tout système aéronautique ayant potentiellement un impact sur la sécurité et nécessitant donc une certification logicielle et matérielle :



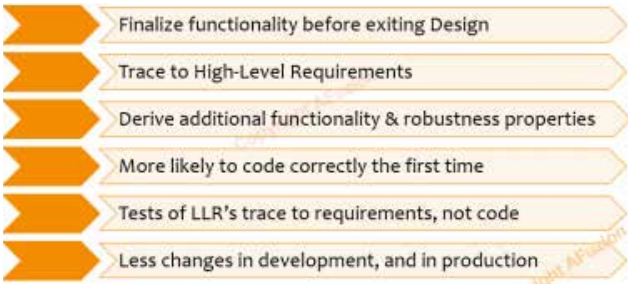

Raisons principales pour élaborer des exigences de haut niveau

Les EHN lient les exigences système aux EBN. De bonnes EHN doivent traiter et clarifier les aspects logiciels suivants :


## Exigences de Bas Niveau

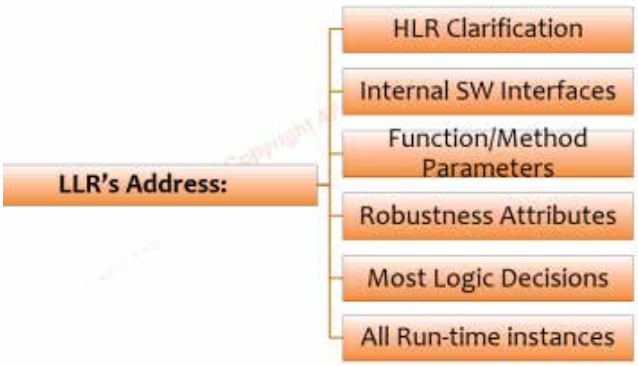
Les EBN suivent la définition des EHN et précèdent ou accompagnent la conception. Les EBN doivent être officiellement revues (voir ci-dessous) avant le développement de la logique associée.

Le graphique suivant met en avant les principales raisons pour lesquelles les EBN sont nécessaires pour tout logiciel d'aéronautique ayant potentiellement un impact sur la sécurité et nécessitant donc une certification logicielle et matérielle :




Raisons principales pour élaborer des exigences de bas niveau

Les EBN lient les EHN à la conception et la mise en œuvre. De bonnes EBN doivent traiter et clarifier les aspects logiciels suivants :

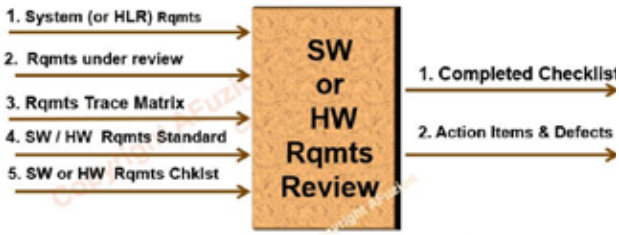



Caractéristiques traitées par les exigences de bas niveau

## Aéronautique : Réparer les Exigences ou Réparer le Produit ?

L'un des aspects essentiels des exigences en aéronautique est la validation précoce. La validation évalue la justesse et l'exhaustivité des exigences. Comme la validation demande de prendre en compte les aspects matériels, les exigences doivent être validées en intégrant les aspects système et matériels. Toutes les exigences doivent être vérifiées. Cette vérification passe par des examens officiels puis des essais. Lorsque les essais ne sont pas concluants, des analyses supplémentaires peuvent être nécessaires. Évidemment, il vaut mieux améliorer les exigences avant la mise en œuvre car la prévention des anomalies est moins coûteuse que leur correction ultérieure. D'un autre côté, la vérification pose la question

suivante : « La mise en œuvre répond-elle aux exigences ? » Toutes les exigences doivent être revues officiellement, ce qui implique l'utilisation démontrable de critères de revue, l'enregistrement et la correction des défauts. À titre d'exemple, les entrées et sorties d'une revue des exigences de logiciel ou de matériel en aéronautique ressemblent à ceci :




*Quelles sont les entrées et sorties d'une revue des exigences ?

Comme présenté plus haut, il y a cinq entrées dans une revue officielle des exigences : il faut que les cinq soient sous contrôle de configuration et il faut prouver qu'elles ont été effectivement utilisées pour effectuer la revue. Ces cinq entrées forment les critères d'entrée, tandis que la checklist de revue des exigences, les mesures à prendre et les anomalies forment les critères de sortie. Ce mouvement d'entrée d'une activité vers la sortie constitue une transition. Le vérificateur des exigences effectue la transition et l'assurance qualité contrôle la transition. Pour les revues, le nombre de contrôleurs est sans importance. Pour les revues des exigences, l'essentiel est d'appliquer le standard correspondant ainsi que la checklist. Les standards adéquats des exigences de sécurité critiques sont détaillés et comptent plus de 20 pages. Quant aux checklists de revue des exigences, elles sont également détaillées et comptent au moins six à huit pages. Cela contraste fortement avec les produits à faible risque pour la sécurité, qui ont rarement des standards d'exigences et des checklists, ou en ont de très légers.

Dans les premières directives en aéronautique, la nécessité et la qualité des exigences étaient reconnues, mais moins appliquées. Les directives modernes exigent un raffinement constant des exigences, de sorte que les défauts et les faiblesses de couverture des tests de logique soient un vecteur majeur dans l'amélioration de la clarté des exigences. DO-178C et DO-278A vont encore plus loin et exigent que les tests pour confirmer la couverture du code logiciel (« couverture structurelle ») soient basés sur les exigences. Cela signifie que les EBN doivent fournir suffisamment de détails pour être utilisées dans les revues de code pour les décisions portant sur la logique.

## Exigences Dérivées

En aéronautique, une exigence *dérivée est* définie comme « une exigence née d'un choix de conception imposant une fonctionnalité ou une capacité particulière qui n'est pas nécessairement liée aux exigences associées ». Les systèmes de sécurité critiques ont presque toujours des aspects qui améliorent la sécurité directement ou indirectement : redondance, tests intégrés, surveillance de la santé, etc. Tous comprennent des

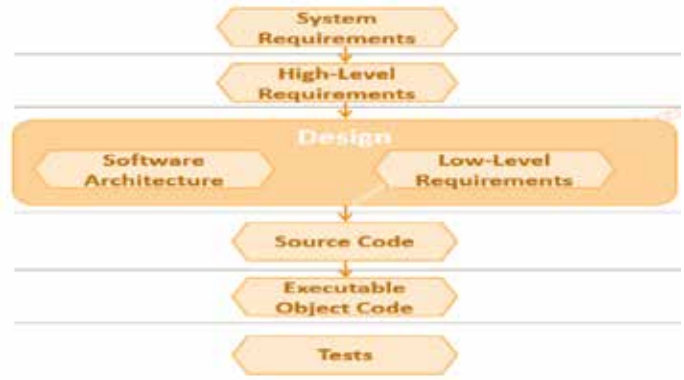
fonctionnalités de sécurité qui ne sont pas nécessairement liées aux exigences. Par conséquent, en aéronautique, ces aspects sont décrits comme des exigences dérivées selon la définition présentée plus haut. Voici des exemples d'aspects d'exigences dérivées :

- Exigences de sécurité telles que la surveillance de l'état de santé pour la réinitialisation, la désactivation ou la commutation.
- Taux d'échantillonnage du système
- Choix d'architecture : redondance triple ou double
- Fréquence d'échantillonnage du chien de garde
- Dissimilarité
- Définition des entrées et sorties matérielles et logicielles

## Exigences = Type de conception = Comment

Tout le monde sait, ou devrait savoir, que les exigences précisent quelle fonctionnalité mesurable est exécutée, alors que la conception précise comment la fonctionnalité est mise en œuvre. Mais prenez un concepteur d'un côté et quelqu'un qui réalise la mise en œuvre de l'autre : le concepteur améliore ses conceptions grâce au prototypage, et le prototypage est une forme de mise en œuvre. Quand quelqu'un modifie la mise en œuvre, il modifie souvent la conception. La frontière entre exigences et conception est floue, ce qui implique une subjectivité vraisemblablement basée sur des suppositions. Pour les logiciels d'aéronautique, embarqués comme au sol, les directives de certification associées DO-178C et DO-278A exigent que l'élaboration des exigences de bas niveau suive l'élaboration des exigences de haut niveau. Les exigences de haut niveau sont toujours dépourvues de détails de conception. Cependant, les exigences de bas niveau font partie intégrante de la conception de logiciels.

Les phases du développement de logiciels en aéronautique sont décrites ci-dessous :




Phases du développement de logiciels en aéronautique

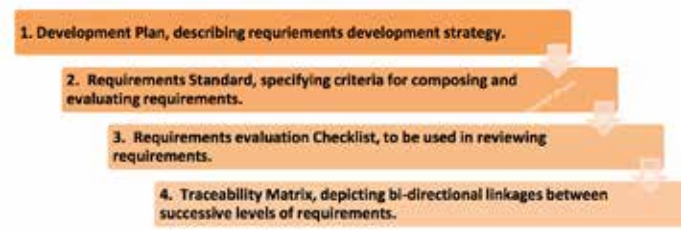
## Créer de Bonnes Exigences et de Bons Standards d'Exigences

À l'instar de tous professionnels, les ingénieurs en aéronautique doivent avoir plusieurs coups d'avance lorsqu'ils créent des exigences. Les exigences en aéronautique doivent être basées sur le résultat final attendu. Là où l'amateur tente à tort de penser aux exigences écrites une par une, le professionnel, lui, doit avoir une vision de la phase finale, c'est-à-dire de l'ensemble des éléments constitutifs d'un système aéronautique performant.

Les directives pour l'aéronautique fournissent très peu d'informations sur la façon d'élaborer des exigences. De ce fait, les méthodes d'élaboration sont très subjectives et donc difficiles à évaluer. Les directives comme DO-178C (logiciels embarqués) et DO-278A (systèmes et logiciels au sol) citent plutôt des « objectifs ». Cela inclut les objectifs d'évaluation des exigences. On les appelle objectifs pour la simple raison que les critères peuvent être appliqués sans ambiguïté. Cependant, les bonnes exigences ont également des critères subjectifs qui ne sont ni demandés ni même traités par les directives pour l'aéronautique.

Dans ce cas, comment les autorités de certification aéronautique vérifient-elles l'inclusion de ces critères subjectifs d'évaluation des exigences ? C'est simple : c'est le but du standard des exigences obligatoires. Les directives pour l'aéronautique exigent que le concepteur crée et applique un standard d'exigences obligatoires pour les niveaux d'assurance supérieurs, autrement dit les niveaux où une défaillance du système pourrait causer des blessures, voire pire.

Revenons-en maintenant à la phase finale : le développement de systèmes aéronautiques performants. Bien que les directives pour les certifications en aéronautique n'exigent pas de méthodologie ou d'approche particulière pour l'élaboration des exigences, le concepteur doit démontrer leur conformité. Ainsi, les directives pour les certifications en aéronautique exigent que les artefacts suivants soient présents avant l'élaboration des exigences :




Entrées requises avant l'élaboration d'exigences conformes

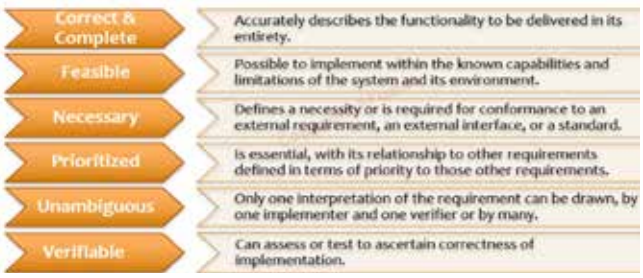
Les quatre entrées pour le processus d'élaboration des exigences en aéronautique ci-dessus doivent être définies avant l'élaboration des exigences. L'évaluation ultérieure desdites exigences doit utiliser ces quatre entrées pour garantir la conformité des processus aux directives. Qu'est-ce qui distingue les amateurs des professionnels dans le monde de l'élaboration des exigences ? Efficacité, précision et qualité :

- **Efficacité** : clarifier les exigences dès le début et avec un minimum d'itérations.
- **Précision** : s'assurer que les exigences sont justes et exhaustives.
- **Qualité** : s'assurer que les exigences sont conformes, qu'elles satisfont à tous les critères de transition (entrées) et sont couplées aux dossiers de revues et d'inspection.

Pour obtenir l'efficacité, la précision et la qualité dans le développement des exigences, il est nécessaire de penser comme des professionnels et de songer d'abord à la phase finale. Pour les amateurs, le but des exigences en aéronautique est de satisfaire les attentes du client en répondant à ses exigences. Pour les professionnels, le but d'un système aéronautique réussi est plus

ambitieux : être conforme à toutes les directives de certification ; satisfaire aux exigences de sécurité et de fonctionnalités, y compris celles du client ; s'interfacer proprement avec d'autres systèmes ; favoriser la réutilisabilité. En d'autres termes, le concepteur d'exigences professionnel a plusieurs coups d'avance et songe à bien plus que la simple satisfaction des besoins du client.

Quelles sont donc les caractéristiques des exigences en aéronautique professionnelle ? Elles sont présentées dans l'illustration suivante :




Caractéristiques des bonnes exigences en aéronautique

## Exigences Faibles

Les exigences faibles sont courantes mais, contrairement à ce que l'on pourrait penser, ne sont pas le fruit d'ingénieurs incompétents ou ignorants. Au contraire, les exigences faibles sont souvent établies à cause d'ingénieurs intelligents convaincus que les exigences sont faites pour les aider. En vérité, les autres ingénieurs doivent être en mesure de lire les exigences pour vérifier les fonctionnalités qu'elles décrivent, ou les modifier ultérieurement. Et ces ingénieurs, peu importe leur intellect, ne connaissent tout simplement pas les exigences aussi bien que la personne qui les a créées.

## Exigences, Objectifs et Désirs Subjectifs

Une erreur courante avec les systèmes de sécurité consiste à décrire des objectifs système comme s'il s'agissait d'exigences. Les objectifs sont comme les bonnes résolutions du Nouvel An : de belles idées potentiellement bénéfiques pour tous. Cependant, les objectifs ne peuvent être évalués et garantis objectivement.

Les objectifs en aéronautique suivants sont trop souvent exprimés sous forme d'exigences :

- « L'aéronef doit être sûr ».
- « Aucun accident grave ne peut se produire ».
- « Les passagers et l'équipage ne peuvent être tués ou blessés ».

Une autre erreur courante consiste à exprimer les exigences par des désirs subjectifs. Les communications humaines sont pétries de désirs subjectifs depuis l'invention de l'écriture. Des mots exprimant les distances (loin, proche), les tailles (grand, petit) et les températures (chaud, froid) apparaissent dans les langues les plus anciennes. Mais leur sens est vague et interprété en fonction du contexte, des préjugés et d'autres facteurs.

Prenez les mots subjectifs suivants, que l'on trouve souvent dans les exigences de sécurité critiques :

- Immédiatement
- Répondre
- Court
- Simultané
- Modulaire
- Nominal

Les mots ci-dessus doivent être remplacés par des termes objectifs pouvant être analysés de manière isolée.

Les exigences suivantes sont un échantillon de ce que j'ai reçu lorsque j'étais cofondateur et CEO de la plus grande société de certification aéronautique au monde. Ce ne sont pas des exigences objectives, ni à peine des objectifs faibles :

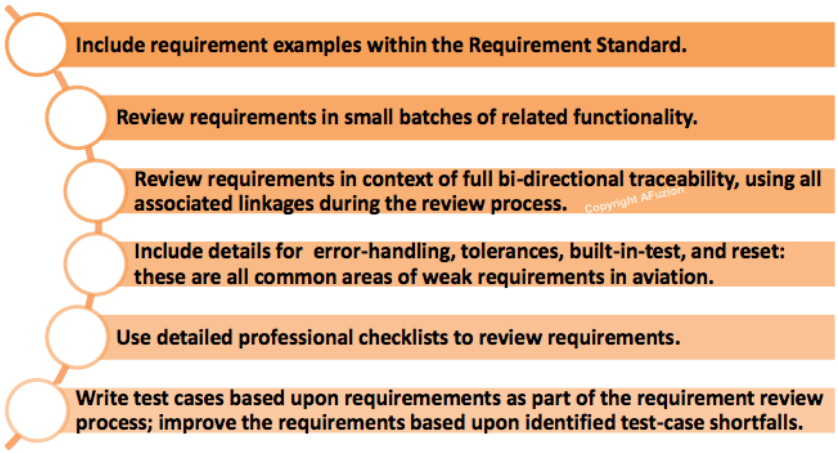
- Le logiciel doit être robuste.
- Le matériel doit se dégrader correctement en cas de contrainte.
- Le logiciel doit être développé selon les pratiques modernes de programmation.
- Le système doit assurer le traitement nécessaire pour tous les modes de fonctionnement.
- L'utilisation de la mémoire de l'ordinateur doit être optimisée pour pouvoir accompagner une croissance future.
- Le logiciel et le matériel doivent être simples d'utilisation.

Un seul mot est valable dans toutes ces exigences : le mot « doit ». Gardez-le et changez tout le reste.

Il est clair qu'il faut un savant mélange de science, d'art, de compétences et de pratique pour élaborer de bonnes exigences. Cependant, il faut aussi des plans, des standards, des checklists et des méthodologies de qualité.

Les bonnes pratiques qui suivent ne font pas partie des directives pour l'aéronautique, car elles ne peuvent être évaluées objectivement, mais elles devraient être intégrées dans le cycle d'ingénierie des exigences :

Bien que ces pratiques ne soient pas obligatoires, quiconque élabore des exigences en aéronautique sans les appliquer, compte sur la chance pour réussir. Les amateurs laissent la chance faire leur succès.




Bonnes pratiques pour l'élaboration des exigences

## À PROPOS DE AFUZION

AFuzion Incorporated est l'une des plus grandes sociétés au monde de services de sécurité critiques, spécialisée dans la formation, l'optimisation des processus, le mentorat, la certification et le conseil, en particulier dans l'aéronautique et l'automobile.

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-178C & DO-254, disponible dans les grandes librairies comme Amazon.com.

En outre, le nouveau 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 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.**