Méthodologie de développement de systèmes critiques

Une approche efficace de l'assurance conception issue du développement de l'aéronautique embarquée

Presenté par James Bezamat

surance conception

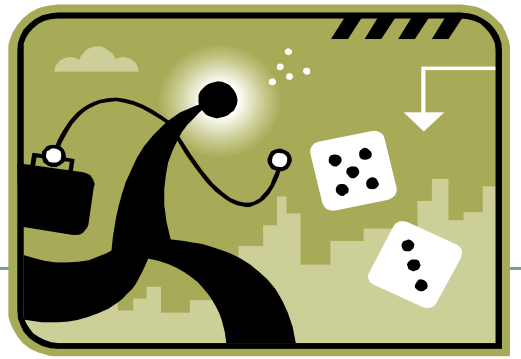
urance Conception (Design Assurance) - Toutes les actions planifiées et matiques utilisées pour justifier, avec un niveau de confiance suffisant, que les rs de conception ont été identifiées et corrigées de telle sorte que le matériel fait aux exigences de certification. ***(DO-254 Appendix C Glossary of terms)***

Il s'agit de démontrer le niveau de sureté de fonctionnement d'un matériel, en s'appuyant uniquement sur l'analyse de son développement et en fournissant le preuves associées, à un regard externe

e méthode de développement rigoureuse et structurée

oyen d'atteindre les objectifs d'assurance qualité du développement :

otée par l'évaluation de la sureté de fonctionnement
nification dès le démarrage du projet de développement
nception orientée processus (structuration)
ntrée sur les exigences, la traçabilité, la preuve de la vérification
proche système et stratégie de passivation des architectures (prise en compte des risques
proche descendante (top down) des exigences (exigences systèmes allouées au matériel)
lisation du savoir faire corporate (référentiel, standards, procédures, bonnes pratiques)
pitalisation sur les projets précédents (relevant history, reuse)
nception à partir de blocs génériques propriétaires (IP) respectant la méthodologie et entièr
montrés

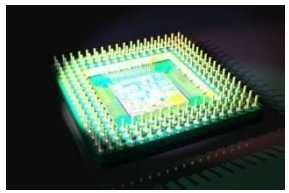


plicabilité

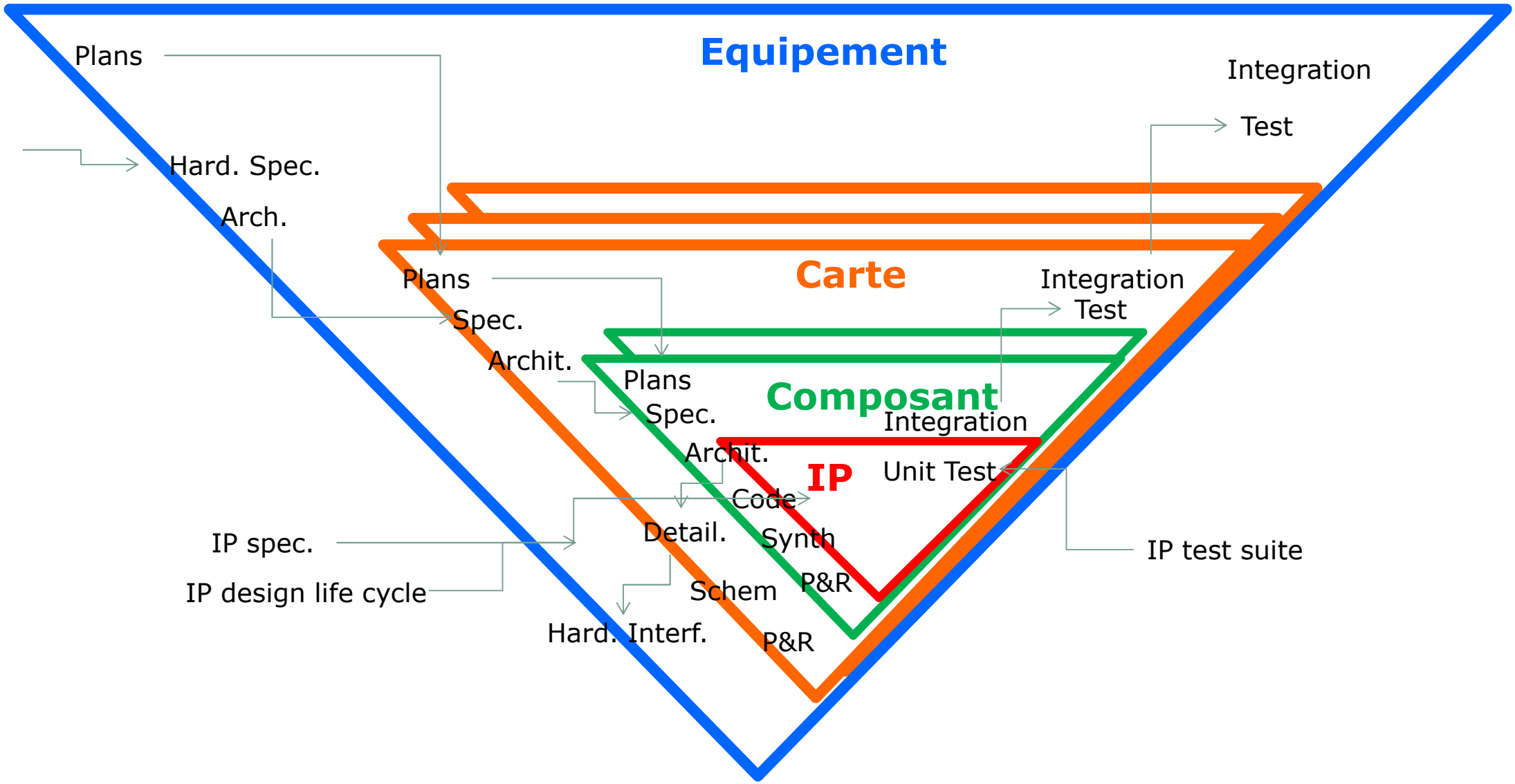
pplicable à tout système, matériel ou logiciel dès lors que l'on peut accéder aux
onnées de conception.

es composants de type COTS (sur étagère) généralement fournis sans ces
onnées de conception nécessitent un traitement particulier (boîte noire) et sont c
éviter au maximum

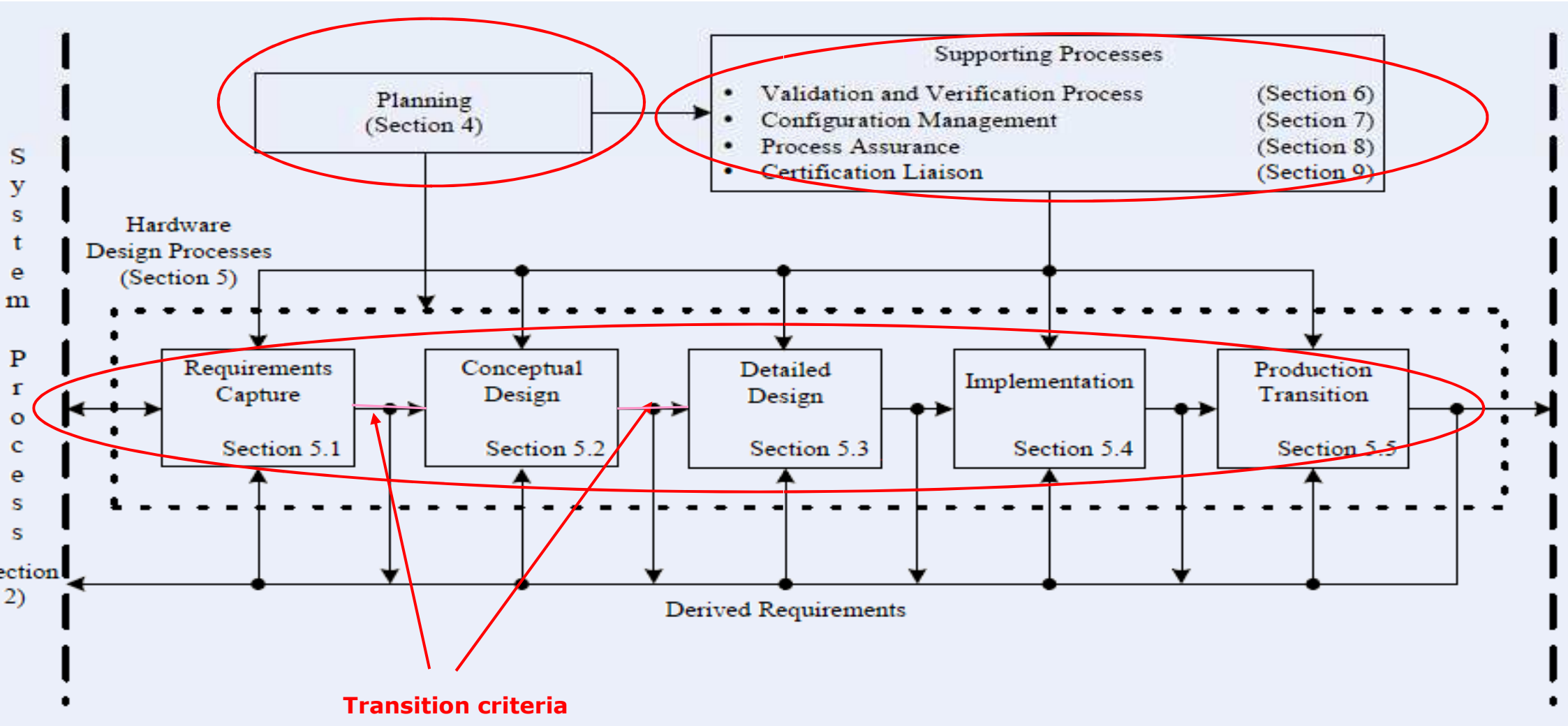
es solutions à base de blocs génériques fournis avec leurs données de concepti
P DO254 compliant) sont préférables, surtout si l'on sait démontrer la validité de
onnées au niveau système (boîte blanche)



e de développement matériel appliqué à tous les niveaux



ocessus du cycle de développement



nification

jectif

finir les moyens par lesquels les exigences fonctionnelles seront converties en
matériel avec un niveau de preuve suffisant de l'assurance que l'item sera capal
réaliser les fonctions attendues de façon sûre.

'agit d'un contrat négocié et approuvé en amont avec les autorités extérieures
(certification)

loit être complet, précis et être rigoureusement suivi.

lécrit l'ensemble des processus, moyens, et l'organisation à mettre en œuvre au
du cycle de développement

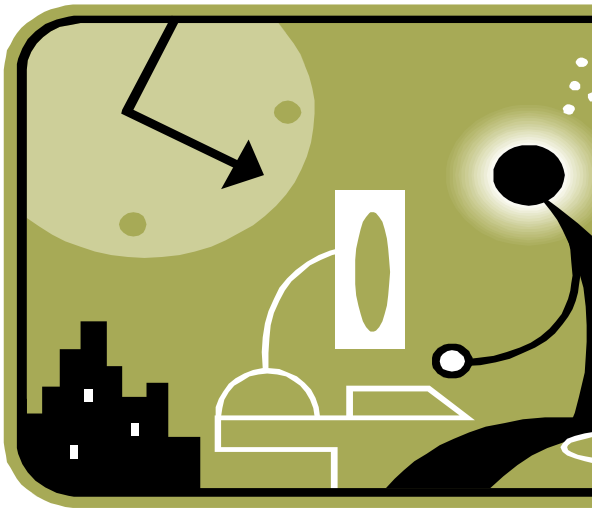
ute déviation sera reportée, justifiée et examinée par les autorités compétentes

The plan is nothing;
the planning is everything
Dwight Eisenhower

pratique

- *Observé*
  - Phase souvent négligée
    - Repoussée à plus tard (le développement avant tout) [perte de temps]
    - Sans réelle réflexion sur la métho (cut and paste)
    - Rédacteur « par défaut » ou pas impliqué
    - Non partagée avec les personnes concernées
  - Décisions tardives
    - Retour client et/ou autorités fortement décalé (le projet est parfois fini)

- *Conséquences*
  - Stratégie non partagée
  - Manque de réflexion (métho, outils, moyens)
  - Acteurs non formés
  - Biais contractuel fort
  - Non respect des plans à justifier en final
  - Perte de temps et d'énergie sans efficacité



- *Parades*
  - Capitalisation sur projets précédents ou accompagnement (premier projet)
    - Mise en place d'une stratégie standard (stable) avec les plans associés
    - Ne reste plus qu'à traiter le différentiel lié au projet
    - Former et informer les acteurs (rôle du chef de projet et de la qualité)
    - Impliquer le donneur d'ordres (kick off, revue de plans)
    - Renforcer le rôle du responsable qualité (garant de l'application des plans)

centre de la méthodologie : les exigences

nsemble de l'édifice méthodologique s'appuie sur la notion fondamentale d'exig

Point d'entrée (contractuel) de tout développement (spécification, top-down)
Référence unique du cycle de conception et du cycle de vérification (fonctionnell
Support de la traçabilité et de la cohérence entre les activités
oint d'entrée de la plupart des activités d'assurance qualité (revue, audit, inspec

ù l'importance d'une parfaite maîtrise de l'écriture de spécification (recueil des exigences) et de l'activité de validation des exigences qui doit s'assurer de la qua et de la cohérence de la spécification.

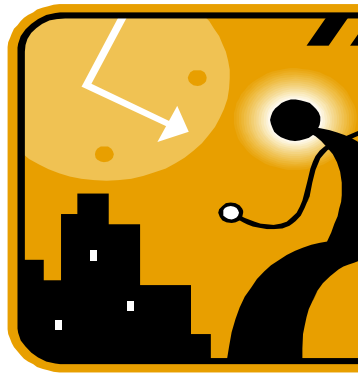
cessité de s'appuyer sur un retour d'expérience fort, une formation des acteurs é éférentiel efficace (templates, checklist)

Requirements are the What.
Design is the How.

pratique

Observé

- Manque de maturité des spécifications (DO et PME)
  - Incomplètes, sous-entendus, ambiguïtés, contradictions
  - Le projet a démarré, la spec est en draft ! Plusieurs versions de la spécification circulent
- Incapacité à écrire une spécification respectant les critères de base
  - Qu'est ce qu'une exigence, quel niveau de précision, est elle vérifiable ?
- Manque de données de justification
  - Traçabilité aléatoire, pas de transparence des décisions, exigences dérivées
- Activité de validation trop faible ou mal conduite
  - Manque d'expertise et de sens critique
  - Activité trop lourde et coûteuse



Conséquences

- Le design commence avec un cahier des charges incomplet, flou et erroné
- Les reprises sont d'autant plus couteuses qu'elles sont tardives et nombreuses
- En cas de problème, détermination des responsabilités impossible : conflits fréquents
- Spécification inutilisable en l'état : retards, incompréhension, non respect des plans et de la métho
- Difficultés lors des audits et de la certification

Parades

- Capitalisation sur projets précédents ou accompagnement (premier projet)
  - Disposer de règles d'écriture de spécification (requirements standard)
  - Mettre en place une activité d'acceptation de la spécification du client (acceptation des entrants, validation de la spécification)
  - Etre ferme avec son donneur d'ordres (la DO254 l'impose, c'est de la qualité base) pour obtenir un point d'entrée utilisable et acceptable
  - Impliquer les acteurs du projet qui vont l'utiliser dans cette phase de validatio (designer, vérificateur) : gain en temps, esprit critique, œil extérieur, préparat des tâches suivantes
  - Etre efficace sur ces activités (rédaction, validation) : appel à des experts, indépendance, outillage, procédures rodées.
  - Y consacrer les efforts nécessaires (mesurer le coût d'une faiblesse à cette étape)
  - Ceci est valable quelle que soit l'activité (hard, soft, système …) : vision corporate et partagée

rification

jectif

montrer que l'objet obtenu est en conformité avec les besoins exprimés au trav
s exigences.

démonstration doit être conduite de façon indépendante (supprimer le biais de
mmun), avec des moyens appropriés et fiables (évaluation des outils), à partir
iquement de la spécification d'entrée (vérification fonctionnelle).

e doit être complète et doit apporter des éléments de preuve (rapports, analyse,
vues). Elle doit démontrer la couverture fonctionnelle de l'ensemble des exigenc

ur les niveaux de DAL élevés il est nécessaire d'apporter des moyens
pplémentaires de vérification (méthodes formelles, analyse structurelle …).

The proof of the pudding is in the eat

pratique

Observé

- Activité subie
  - Importance non saisie (historique électronique simple et reprogrammable)
  - La DO254 l'impose donc je le fais, mais je suis persuadé que cela est inutile
- Difficulté à assurer l'indépendance
  - Petite équipe, manque de personnel compétent
  - Historique contraire (le designer est responsable de la totalité du développement)
- Activité sous évaluée (en temps et en ressource)
- Sous-traitance pas toujours maîtrisée

Conséquences

- Résultats non satisfaisants (un des points de sorties les plus examinés)
- Dépassements de temps et de budget
- Sous-outillage (souvent gratuit, mais insuffisant)
- Non exhaustivité et déficit de preuves
- Bugs plus nombreux, plus tard, responsabilité complexe à établir
- Impossibilité d'évolution et de capitalisation

pratique

Parades

- Si le manque de ressource, taille de l'équipe, investissement outils sont les problèmes : faites appel à la sous-traitance.
- Comme pour le design, disposer de bonnes pratiques internes, de règles d'écritures, de procédures standardisées, de bibliothèques de fonctions.
- Bien gérer l'indépendance (même pour des niveaux de DAL faibles) qui perm de mener les activités design et vérification en //.
- Utiliser efficacement la vérification pour remonter rapidement les bugs et dysfonctionnements
- Systématiser les revues et les audits qui permettent de s'assurer de la qualit processus de vérification (traçabilité, couverture, pass/fail criteria, rapports).

cessus support : gestion de configuration, suivi des évolutio

jectif

surer la transparence totale et la reproductibilité de l'ensemble des activités du
développement. Identifier de façon unique les données manipulées.

e capable de justifier n'importe quelle intervention (modification, correction,
olution, mise au point, reprise) sur une donnée (technique ou documentaire) du
base de tout audit externe)

surer la cohérence et l'exactitude des données utilisées lors d'une revue, d'une
ase de vérification, d'un transfert vers la production (baseline)

montrer le respect du processus de gestion des erreurs et évolutions (Problem
port, Change Request tracking) tel que décrit dans les plans.

cessité d'un outillage puissant, cohérent (2 outils), intégré, personnalisé en fonc
la méthodologie, facile à utiliser, sûr et fiable

pratique

Observé

- Activité subie (par les ingénieurs)
  - Pas expliquée, pas formés, pas sensibilisés à l'importance du processus
- Activité réservée au développement software
  - Pas dans les mœurs des équipes hardware, surtout dans les PME
- Réservé aux gros projets très complexes, longs et multi sites (l'exception dor
- Croyance aveugle dans l'outil, au détriment de la façon dont on l'utilise
  - En l'occurrence les outils open source sont souvent aussi efficace (bien utilisés)
- Aucune liaison entre gestion de configuration et gestion des problèmes
- Syndrome Excel et/ou Zip pour répondre à tous les besoins

Conséquences

- Audits catastrophiques
- Failles dans le suivi et la justification des évolutions (documents). Reuse en péril
- Défauts de cohérence des données (N versions sur M postes) : risque fonctionnel grave
- Dénote une non-maîtrise du processus de conception : faute rédhibitoire aux yeux de la certificatio

pratique

Parades

- Des outils simples en nombre limité.
- Une configuration performante, efficace et utilisable (le cœur d'un écosystèm
- Des utilisations maîtrisées, décrites et partagées (dans les plans)
- Des workflows adaptés à chaque besoin
- Des utilisateurs sensibilisés et formés
- Etre irréprochable (avoir en tête l'audit de certification en permanence)
- Ne pas tricher (une reprise avouée est pardonnée, un défaut masqué se voit premier coup d'œil)
- Des rôles bien compris et clairement définis
- Réfléchir avant toute chose (stratégie, justification, traçabilité)
- Un travail d'équipe efficace et rapide (nombre d'intervenants successifs important)
- Tout le monde doit être capable de démontrer n'importe quel aspect de la gestion de configuration : réussite assurée

surance qualité

jectif

rance processus garantit que les objectifs des processus du cycle de vie ont été
its et que les actions ont été accomplies conformément aux plans ou que les
ions ont été traitées. *(DO-254)*

uie sur des activités de revue et d'audit menées de façon indépendante, avec le
rt de checklists dédiées.

ponsable Assurance Process agit au cœur du projet. Il participe aux revues
ncement, aux revues de pairs. Il est techniquement compétent.

ouve les documents, il clôt les actions (PR), il s'assure de la qualité des sous-tr
interface avec les donneurs d'ordres et les autorités de certification.

rise la transition entre processus et il certifie le résultat final (First Article Inspect

Review is not necessarily the best time
discover the user requirements.
Alexander's 18th Law

pratique

Observé

- Activité fortement subie (par les ingénieurs et l'encadrement)
  - « Le responsable qualité est dans le projet pour l'empêcher d'avancer »
  - « il vient critiquer une fois les travaux terminés », « la qualité n'a jamais fait voler un avion »
- Pas de service qualité/ manuel qualité (ou pas adapté)
- Pas de culture qualité dans l'entreprise, pas d'indépendance de la qualité
- Activité lourde et inutile
  - Des revues, encore des revues, toujours des revues, pour quoi faire ?
  - Responsable de la mise en place de tous ces processus « administratifs » qui nous empêche de f code
  - La qualité recherche la petite bête pour trouver le prétexte pour stopper le projet
- Trop souvent calqué sur une activité qualité « traditionnelle »
  - Assez loin du quotidien du projet,
  - Pas forcément une compréhension technique suffisante

Conséquences

- Incapacité à démontrer la qualité du travail, le respect des plans.
- Un développement sans garde fou extérieur : risque accru et non maîtrisable

pratique

Parades

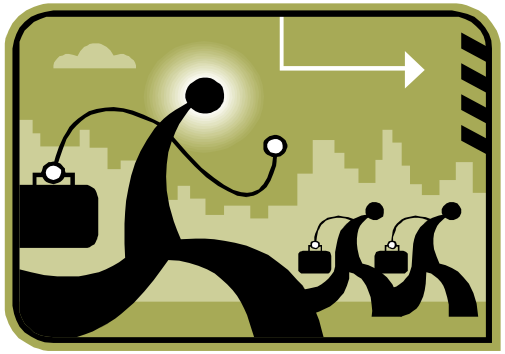
- La qualité est un élément à part entière du projet
- Elle est l'affaire de tous et est gérée par une personne indépendante, efficace compétente et au service du projet
- La qualité se planifie, se prépare, s'appuie sur des compétences et est régie des processus type ISO9100 ou autres (vision corporate)
- Elle est précise, adaptée aux attentes projets et aux attentes DO254
- Elle dispose de moyens performants (templates, checklists de revues, d'audi
- Elle démontre son efficacité aux autres acteurs
- Elle dispose d'une autorité forte (signature) et d'une sagesse infinie (rare)
- Le chef de projet et le responsable qualité forme une équipe qui partage beaucoup d'activités avec des rôles et prérogatives différentes (parfois opposées) : le secret d'un projet qui fonctionne

-254 complaints

ntendu

Charge de travail supplémentaire sans réelle valeur ajoutée

- Documents additionnels
  - Perte de temps à écrire des documents formels
  - Le temps consacré au travail « réel » est inférieur à 10%
  - Relecture et audits sont totalement improductifs
- Nombreuses revues
  - A chaque étape, ralentit l'avancement d'un projet



2. Problèmes de management

- Trop d'intervenants
- Dépassement de délai
- Pas le temps de tout faire (DO254 pas négocié)
- Tentation du bypass pour répondre aux pressions du client

3. Impact des changements, évolutions, reprises, corrections de bug

- Un changement mineur peut avoir des conséquences lourdes (documentaires, revues, vérifica
- Pas le temps de tout faire

nclusion optimiste

Tout ce que demande la méthodologie devrait de toute façon être fait par l'équipe projet.

Les processus et les standards utilisés sont issus des bonnes pratiques de l'entreprise devraient être utilisés dans tous les projets.

En adoptant cette approche on évite :

- Travail en double
- Discussion sans fin autour de la spécification
- Problèmes ouverts et jamais clos
- Surcoût imprévus à la fin du projet (qui ne respecte pas la spécification)
- Défauts cachés

En adoptant cette approche on y gagne :

- Projets plus prévisibles (déterministes ?)
- Management maîtrisé
- Designs plus fiables, robustes : production et maintenance facilitée
- Confiance dans le résultat, dans le produit (fidélisation client)
- Réutilisation et évolutivité améliorée