Making Ideas a Reality

SEE
Certification et Méthodes Formelles
Toulouse, 3 février 2004

Pierre Morère
Responsable Ada et Safety

Présentation

- Evaluateur Certifer pour des projets ferroviaires
  - EN50128 SIL4
  - TGV Espagne
  - Principalement Ada83 sur cible 68k
- Evaluateur pour la SNCF sur le projet CTRL
  - Divers niveaux de certification
- Participation à différentes études de sécurité
  - diversification de code
  - réduction des temps de validation
- Pour Aonix
  - Support pour les audits Safety sur les noyaux C-SMART et Raven
  - Développement de BSP SIL 4 EN50128

Suivi documentaire (1)

- Petit projet
  - Jusqu'à 4 versions de certains documents
  - Evaluation s'étendant sur plus de 18 mois
  - Environ 80 documents liés au logiciel
  - Code + scénarii de tests (unitaires, intégration, validation)

PB 1 => vérifier la cohérence entre l'ensemble des documents et ne pas perdre pieds

Suivi documentaire (2)

- Gros projet
  - Jusqu'à x versions de certains documents
  - Evaluation s'étendant sur plus de x mois
  - Documents * nombre de sous-systèmes
  - Documents fournis soit au fil de l'eau, soit par lot.

PB 2 => le cycle en V n'est pas forcément respecté

PB 3 => cycle de développement d'un système complet non spécifié

Produits génériques

- Un produit générique
- Un paramétrage (en général par les données)
  - première certification au travers d'un seul paramétrage
- Plusieurs projets
  - liens entre les projets
  - évolution minime

PB 4 => garantir la sécurité quelque soit le paramétrage

PB 5 => évaluation par delta

PME/PMI

- 2 comportements distincts lors de la première certification
  - Sous-estimation des coûts
    - Syndrome “Ca marche”
  - Mise en place d’un système trop rigide
    - Syndrome “Ceinture et bretelles”

PB 6 => Certification peut s’avérer très pénalisante financièrement

Pertinence des campagnes de tests

- Tests unitaires
  - Entrée des scripts de tests
  - Vérification des scripts de tests

PB 7 => tests de couverture structurelle essentiellement

Utilisation des COTS

- EN50128 pas vraiment explicite
- Utilisation des COTS pour du SIL4 plutôt récente
- Dépend fortement de la culture du pays

PB 8 => harmonisation nécessaire entre les organismes évaluateurs.

Niveaux inférieurs

- Difficulté pour évaluer du SIL2 ou Niveau C
- Que peut-on utiliser?
  - Windows NT?

PB 9 => on voit de tout

Problème de disponibilité

- La plupart des problèmes trouvés en évaluation sont de disponibilité

PB 10 => impact de la disponibilité d'un sous-système sur le système global

Preuve formelle

- Utilisation d'outils, de méthode garantissant un certain niveau de confiance
  - vérification de règles de codage
  - méthode B
  - PolySpace
  - Simulation de modèles

PB 11 => mise en place de la stratégie des dominos

Performance

- Utilisation de méthode de développement sûre
- Validation très tôt du logiciel
- Modification du code généré ou prouvé pour tenir compte de problèmes de performance

PB 12 => risque de remise en cause de la sécurité

On n’a pas un métier facile

- Contraintes industrielles
- Contraintes financières
- Compétences variées et incomplètes
- Normes améliorables