Les standards
et la prise en compte des COTS :

comment se concilient l'utilisation des COTS et les normes actuelles ?

Marie-Hélène Durand

Aerospatiable Matra Airbus et LIS

Plan

- Introduction
- Domaine Aéronautique
- Domaine Ferroviaire
- Domaine Nucléaire
- Domaine Militaire
- Norme Européenne CEI 61508
- Des points communs
- Des ouvertures
- Concilier les normes actuelles avec l'utilisation des COTS dans les systèmes critiques ?

Introduction

- Plusieurs normes abordent la notion de COTS ou plus généralement de composants développés antérieurement (PDS, LPD ...)
- Plus les normes sont récentes, plus les COTS y sont présents
- Parcours des exigences de 9 documents:
  - Aéronautique Civile — DO178B, Do254
  - Domaine Ferroviaire — CENELEC prEN50128
  - Domaine Nucléaire — CEI 60880 et son supplément, CEI 61513/CDV
  - Domaine Militaire — Def Stan 00-56, Def Stan 00-55
  - Norme Européenne — CEI IEC 61508 (Parties 2 et 3)

Domaine Aéronautique (1/2)

DO178B/ED12B : « Considérations sur le logiciel en vue de la certification des systèmes et équipements de bord »

Les exigences du DO178B applicables aux logiciels développés spécifiquement, doivent être appliquées à tous les COTS ou composants intégrant des COTS

(Exigences fonction du niveau logiciel attribué selon le processus d'évaluation de la sécurité)

- **Evaluation des données existantes**
- **Rétro-ingénierie ou vérification complémentaire pour générer les données inadéquates ou manquantes** (accès à la conception, au source …)
- **Possibilité de prendre en compte l'historique en service du produit :**
  - Analyse de la représentativité de l'environnement par rapport à l'utilisation prévue
  - Evaluation précise de la période de service avec justifications
  - Enregistrement complet et analyse systématique des anomalies
  - Définition de ce qui est comptabilisé comme une erreur ou non, ainsi qu'un taux de défaillance acceptable
  - Gestion de la configuration du produit et de sa documentation

Domaine Aéronautique (2/2)

DO254/ED80 : « Design assurance guidance for airborne electronic Hardware »

Crédit de certification possible si l'on peut établir :

- La démonstration d'un processus de contrôle qualité, et de l'enregistrement et analyse des anomalies, chez le fabricant
- Le contrôle du niveau de qualité du composant, établi chez le fabricant ou par des tests supplémentaires
- La fiabilité du composant établie lors de la qualification, et la surveillance continue de la fiabilité et de la performance du composant
- L'historique en service d'une utilisation opérationnelle satisfaisante:
  - Taux de panne observé acceptable
  - Similarité d'utilisation en terme de fonction, d'environnement opérationnel et de niveau d'assurance conception
  - Traitement des erreurs de conception, et historique des modifications
- L'analyse de l'impact du composant sur la sécurité
- Des moyens supplémentaires d'assurance pour les niveaux A et B

Domaine Ferroviaire

CENELEC pr EN50128 (draft final): « Software for Railway Control »

Utilisation des COTS soumise à quelques exigences fonction des niveaux de sécurité des logiciels (niveaux de 4 à 0, 4 étant le plus critique), et basées principalement sur l'analyse de défaillances potentielles du COTS et les protections implantées

- **Niveau 0 :**
  - pas de précaution
- **Niveaux 1 ou 2 :**
  - COTS à inclure dans le processus de validation
- **Niveaux 3 ou 4 :**
  - COTS à inclure dans le processus de validation
  - Analyse des défaillances potentielles du COTS
  - Stratégie de détection des défaillances et de protection du système (à définir et valider)
  - Enregistrement et analyse des défaillances
- **Pour un LPD (Logiciel Développé Précédemment):**
  - Le LPD doit être identifié et documenté
  - Le LPD doit satisfaire aux spécifications et au niveau de sécurité logiciel requis
  - Toute modification doit être analysée pour décider d'une éventuelle ré-inspection ou réévaluation
  - Le LPD doit remplir les spécifications des interfaces des composants non re-vérifiés

Domaine Nucléaire (1/3)

CEI 61513/CDV (draft): Exigences applicables aux systèmes d'instrumentation et de commande utilisées pour la sûreté dans les centrales nucléaires

Les exigences applicables sont fonction de la classe du système.

Pour la classe 1 (la plus critique), les composants préexistants doivent être développés selon les normes CEI du secteur nucléaire

- **Classe 2: COTS sélectionnés et qualifiés (développés selon des directives reconnues, ou provenant de composants qualifiés antérieurement avec historique et fonctionnement similaire satisfaisant)**
- **Classe 3: COTS sélectionnés**
- **Exigences:**
  - **Documentation comportant la fonctionnalité et les propriétés de tous les composants (taux de défaillances, conditions environnementales …)**
  - **Propriétés non explicites à déterminer par une analyse ou un essai**
  - **Identification des fonctions des composants non utilisées, et démonstration que ces fonctions ne peuvent compromettre les fonctions requises**
  - **Détermination de la fiabilité et de la performance des fonctions d'applications de la centrale dans les configurations anticipées**

Domaine Nucléaire (2/3)

CEI 60880 1er suppl. (draft 10/05/99): Exigences applicables à l'utilisation de Logiciels Pré-Développés dans les systèmes de sûreté des centrales nucléaires

4 étapes pour l'évaluation et l'agrément d'un LPD:

- **1 - Evaluation des fonctions et performances du LPD, ainsi que de la documentation existante :**
  - Approche « boite noire »
  - Document de Spécifications et document utilisateurs du LPD
  - Spécifications système donnant les exigences d'interface et de performance pour le LPD
  - Identification des fonctions non utilisées du LPD et les mesures pour éviter les interférences de ces fonctions avec les fonctions de sûreté
- **2 - Evaluation de la qualité de la conception et du développement du LPD, ainsi que de l'appropriation à l'usage :**
  - Approche « boite blanche »
  - Démonstration que le LPD est conforme aux exigences d'un système qui réalise des fonctions de catégorie A
  - Documents, ou informations alternatives: conception, code source, documents de vérification, plan qualité ...
  - Fourniture de la documentation de l'historique en service pour compenser des manques

Domaine Nucléaire (3/3)

CEI 60880 1er suppl. (draft 10/05/99): Exigences applicables à l'utilisation de Logiciels Pré-Développés dans les systèmes de sûreté des centrales nucléaires

- **3 - Evaluation de l'historique en service :**
  - **Validation des méthodes de collecte de données (fournisseur et si possible utilisateurs):**
    - Processus de collecte bien défini et contrôlé
    - Validation de l'exhaustivité et de la crédibilité des données
    - Prise en compte de l'expérience en service seulement dans des conditions similaires
    - Calcul du temps d'exploitation cumulé du LPD (pour des LPD de même version); pour des LPD de versions différentes, les historiques et les différences doivent être analysés
    - Analyse et classement des défaillances en fonction de leur sévérité
  - **Critères de validation de l'historique en service :**
    - Temps d'exploitation suffisant
    - Ni modification importante, ni erreur importante, détectée sur une période significative et sur plusieurs implantations
- **4 - Agrément de la qualité des preuves suite à l'évaluation et aux travaux supplémentaires associés :**
  - **Justification de l'utilisation du LPD dans le système**
  - **Historique en service analysé pendant toute la durée du cycle de vie du système**

Domaine Militaire (1/2)

Def Stan 00-56/Issue2 : « Safety management requirements for defence systems » (Ministry of Defence of UK)

Une évaluation de la conformité aux objectifs de sécurité doit être menée pour tout NDI (Non Development Item) ou système hérité

- **Etablir la base des documents disponibles**
- **Identifier toutes les non conformités au standard Def Stan 00-56**
- **Rassembler diverses informations:** standards utilisés, analyses de sécurité existantes, historique (accidents, anomalies, modifications …) du composant, rôle du composant dans les accidents, certification …
- **Mener des analyses supplémentaires (rétro-ingénierie éventuelle) ou utiliser l'historique en service, et démontrer que le composant atteint les objectifs de sécurité**
- **Rédiger un Plan Qualité Projet et disposer d'une gestion de configuration**
- **Produire un rapport contenant les règles de conception, techniques, standards utilisés pour les systèmes hérités**
- **Faire une analyse de risque au niveau système, avec estimation d'une probabilité de risque**

Domaine Militaire (2/2)

Def Stan 00-55/Issue2 : « Requirements for safety related software in defence equipment » (Ministry of Defence of UK)

Le PDS (Previously Developed Software), ses modifications éventuelles et sa documentation, doivent être démontrées conformes aux exigences du standard Def Stan 00-55/Issue2, et n'affectant pas la sécurité du système

- **Pour un PDS non conforme, une rétro-ingénierie, et des activités de vérification et de validation seront menées selon les exigences de sécurité, l'existant, le niveau logiciel du PDS et son historique en service**
- **Pour tout code du PDS non activable et conservé, on montrera que laisser ce code présente moins de risque que de l'enlever**
- **L'historique en service n'est utilisable que si des données fiables concernant l'usage et les taux de défaillance du PDS existent:**

  Gestion de configuration, exhaustivité des rapports d'anomalies, impacts des anomalies, similarité entre les environnements des utilisations passées et celui de la nouvelle application, taux de défaillance quantifié, durée très précise des périodes de service

Norme Européenne CEI IEC 61508

Les COTS sont peu abordés

Partie 2 : « Requirements for electrical/electronic/programmable electronic systems » (Draft version 2.3 du 11/12/96)

Pour les applications sécuritaires :

- Composants COTS devant être clairement identifiés et documentés
- Si la documentation est insuffisante, l'historique en service peut être utilisé :
  - Justification précise de l'utilisation
  - Justification d'une utilisation opérationnelle dans une application similaire, ou démonstration que le composant COTS satisfait les exigences

Partie 3 : « Prescriptions concernant les logiciels » (1ère édition 1998)

- Logiciels COTS devant être clairement identifiés
- Justification de la capacité de ce logiciel COTS à satisfaire les exigences de sécurité
- Fonctionnement satisfaisant dans une application similaire, ou application des mêmes exigences de vérification et de validation que pour un logiciel nouveau
- Evaluation des contraintes imposées par les environnements précédents

Des points communs

- Exiger la conformité des COTS à toutes les exigences des composants développés spécifiquement, particulièrement pour les systèmes critiques
  - ⇨ Analyse boite blanche du COTS
  - ⇨ Activités complémentaires de vérification, de rétro-ingénierie; nécessité d'obtenir le code source (pas toujours contractuellement possible)
- Identifier les fonctions du COTS non utilisées, et les mesures prises pour que ces fonctions n'interfèrent pas avec les fonctions utilisées
- Utiliser l'historique en service pour compenser les non-conformités mais avec des contraintes strictes pas toujours possibles :

  Gestion de configuration, exhaustivité des rapports d'anomalies, analyse des impacts des anomalies, taux d'erreur quantifié, calcul précis de la période de service, adéquation des environnements d'utilisation passés du COTS avec celui de la nouvelle application … (stratégie non nuancée selon le niveau de sécurité du système)

Des ouvertures

- Utilisation de l'historique en service, mais les contraintes sont assez strictes
- Quelques stratégies plus ouvertes ou plus « quantifiables » pour les composants matériels (exemple le DO254)
- Pour le ferroviaire, insistance des exigences sur l'analyse des défaillances potentielles du COTS, et l'étude et la validation de la protection du système contre ces défaillances

  Donc une approche basée davantage sur les conséquences de l'intégration du COTS sur la sécurité (au sens « safety ») du système

Concilier les normes actuelles avec l'utilisation des COTS dans les systèmes critiques ?

Les normes actuelles sont peu adaptées à l'intégration de COTS « boite noire » dans les systèmes critiques

- **Analyser les techniques de validation d'un COTS**
- **Analyser les techniques architecturales (empaquetage …) et donner des règles de conception d'une architecture intégrant des COTS**
- **Analyser les différents aspects du cycle de vie influencés par l'introduction d'un COTS (sélection, développement, obsolescence, aspects contractuels, gestion de configuration …)**
- **Emettre des recommandations quant aux solutions potentielles et l'utilisation de l'expérience en service**