C8 - Sureté et Fiabilité des Systèmes Critiques

Objectifs

- Comprendre les enjeux de la sécurité de fonctionnement
- Découvrir les méthodes de preuves formelles
- Appréhender les normes de développement applicables
  - IEC 61508
  - DO-254
  - DO-178B et C
- Comprendre le processus de certification

Pré-requis

- Connaissance de base de la réalisation de systèmes embarqués et temps-réel

Environnement du cours

- Cours théorique
  - Support de cours imprimé et au format PDF (en anglais).
  - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique.
- Au début de chaque demi-journée une période est réservée à une interaction avec les stagiaires pour s'assurer que le cours répond à leurs attentes et l'adapter si nécessaire

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Modalités d'évaluation

- Les prérequis indiqués ci-dessus sont évalués avant la formation par l'encadrement technique du stagiaire dans son entreprise, ou par le stagiaire lui-même dans le cas exceptionnel d'un stagiaire individuel.
- Les progrès des stagiaires sont évalués par des quizz proposés en fin des sections pour vérifier que les stagiaires ont assimilé les points présentés
- En fin de formation, une attestation et un certificat attestant que le stagiaire a suivi le cours avec succès.
  - En cas de problème dû à un manque de prérequis de la part du stagiaire, constaté lors de la formation, une formation différente ou complémentaire lui est proposée, en général pour conforter ses prérequis, en accord avec son responsable en entreprise le cas échéant.

Plan

Premier Jour

Sécurité de fonctionnement

- Analyse des risques

- Techniques d analyse
  - Modes de défauts et analyse des effets
  - Analyse de l arbre des défaillances
- Certification de la sécurité
- Technique de prévention des défaillances
  - Systèmes à sécurité inhérente
  - Limitation de l effet des défaillances
- Sécurité et fiabilité

Preuves formelles

- Nécessité d une spécification formelle
- Méthodes de spécifications formelles

Exemple : : *les preuves par invariants, pré et post-conditions*

Les normes de la sureté de fonctionnement logiciel

- Norme CEI 61508
  - Les niveaux d intégrité de sécurité (SIL 1 à 4)
  - Validation
- Norme DO-178 (B & C) et DO-254
  - Les niveaux de criticité (A à E)
  - Qualification des outils
- Les autres normes

Second Jour

Le processus de certification

- Organismes de certification
  - FAA
  - AESA
  - JAA
  - &
- Procédures de certification
- Différents type de certificats
  - Type Certificate (TC)
  - Supplemental Type Certificate
- Les TSO (Technical Service Order)
- Le rôle des DER (Designated Engineering Representative)
  - Différence entre la FAA et l AESA
- Le chemin vers une certification réussie

La norme DO-178B

- Le modèle de développement DO-178B
  - DO-178B et DO-254
  - Le cycle en fuseau
  - Les processus du cycle de vie
  - Différence entre vérification et test
- Le processus de développement
  - Support au développement
  - Développement
  - Assurance qualité
  - Certification
- Le cadre de vérification
  - Revues
  - Analyses

  - Tests
- La traçabilité des exigences
  - Liens avec les tests
  - Couverture de tests
- DO-178B et produits sur étagère

Troisième Jour

La norme DO-178C

- Pourquoi une nouvelle norme
  - Objectif de la DO-178C
  - Stratégie de définition
  - Structure de la norme DO-178C
- Les différences par rapport à la DO-178B
  - Clarifications de la norme
  - Changements apportés au Coeur du codument
  - Nouveaux elements
- Les suppléments
  - DO-330 : Qualification des outils
  - DO-331 : Développement par les modèles
  - DO-332 : Technologies objet
  - DO-333 : Méthodes formelles

Renseignements pratiques

Durée : 3 jours
Prix : 2400 € HT