Sûreté de fonctionnement et risques logiciels, AMDEC du logiciel et AEEL

Cours Pratique de 3 jours - 21h
Réf : SUF - Prix 2024 : 2 180€ HT

Ce stage vous montrera comment mettre en œuvre les techniques d'analyse de risque et de fiabilité/disponibilité du logiciel. Par des réalisations concrètes sur des cas pratiques, vous apprendrez à utiliser les principaux référentiels et outils conceptuels du domaine : CEI 61508, ISO 26262, STD 882E, AMDEC, AEEL, COTS.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les principes et la démarche d'analyse de risque et de fiabilité du logiciel

Appréhender les étapes et les composants d'un dispositif de Sûreté de Fonctionnement du logiciel

Analyser un programme, afin de vérifier les règles de codage, dans une optique de fiabilité du logiciel

Réaliser une analyse des Effets des Erreurs de Logiciel (AEEL), en appliquant la démarche phase par phase

MÉTHODES PÉDAGOGIQUES

Cours et mise en pratique via des exercices et des études de cas. Les exercices proposés sont représentatifs des problématiques rencontrées sur le terrain.

EXERCICE

Des cas concrets pour illustrer les concepts de fiabilité du logiciel et d'AEEL.

LE PROGRAMME

dernière mise à jour : 08/2023

1) Concepts et principes de la SdF du logiciel

- Le champ d'application de la SdF et les enjeux.
- Définition du risque.
- Principales caractéristiques.
- Nature des exigences pour le logiciel.

Travaux pratiques : Identification des principales exigences de Sûreté de Fonctionnement du logiciel.

2) Enjeux et problématiques de la SdF du logiciel

- Construction et terminologie de la SdF du logiciel.
- Assurance de la SdF.
- Le Plan de SdF. Les éléments constitutifs.

Travaux pratiques : Construction de la Sûreté de Fonctionnement du logiciel.

3) Etude système

- Sécurité innocuité.
- Attribution niveau SIL (selon CEI 61508).
- Notion d'indépendance (selon CEI 61508, ISO 26262).
- Exigence SdF. Exigence fiabilité.

Travaux pratiques : Spécification d'une fonction de sécurité selon CEI 61508.

PARTICIPANTS

Développeurs, chefs de projets, responsables de validation confrontés au développement de systèmes critiques faisant appel à une forte composante logicielle.

PRÉREQUIS

Connaissance des méthodes et outils de développement informatique. Connaissance des processus de développement des systèmes programmés.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

4) Fiabilité du logiciel

- Définition. Les déclencheurs et entrants à la fiabilité du logiciel (normes et référentiels). Métrologie.
- Les différents types de logiciels.
- Pourquoi et quand évaluer la fiabilité ? Exemples.
- Fiabilité expérimentale, sa mise en œuvre.

Travaux pratiques : Estimation de la fiabilité d'un logiciel.

5) Sécurité (innocuité) du logiciel

- Barrière de sécurité.
- Démarche selon la norme CEI 61508.
- Démarche selon la norme STD 882E.

Travaux pratiques : Programme de sécurité (innocuité) selon STD 882E.

6) AMDEC

- Théorie de l'AMDEC du logiciel : analyse des modes de défaillance, de leurs effets et de leur criticité.
- Les analyses phase par phase.
- L'analyse des mécanismes de défaillance.
- L'évaluation de la criticité.
- Les propositions d'actions correctives.
- La présentation et l'interprétation des résultats.
- AMDE du logiciel.
- Différence avec l'AEEL (Analyse des Effets des Erreurs de Logiciel).

Travaux pratiques : Réalisation d'une analyse AEEL.

7) COTS

- Intégration de composants COTS.
- COTS pour les systèmes critiques (sécurité innocuité).
- Exemple d'un processus d'étude de sécurité intégrant un COTS.
- Dispositifs architecturaux.

8) Conclusion

- Les aspects normatifs. Les pratiques industrielles.
- Les principales limites de la méthode AMDEC.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 03 juil., 30 sept., 09 déc.	2024 : 26 juin, 23 sept., 02 déc.