Designing for safety

ECTS
4 crédits

Volume horaire
42h

Présentation

Description

UE 3 : Développement de systèmes sûrs « Designing for safety » présente comment la sécurité doit être prise en compte dans le processus de conception d'un système en abordant les risques inhérents aux dysfonctionnements des systèmes, ainsi que les démarches, les modèles et les techniques d'identification, d'analyse et de traitement des risques liés aux fautes de conception et à la fiabilité des composants.

Responsable de l'UF : Jean-Charles Fabre.

Partie 1 : Motivations et introduction des 4 types de dangers « système »

Motivation : Importance croissante des systèmes sociotechniques au cœur de la société comme source potentielle de dommages ; Responsabilités de l'ingénieur et objectifs de l'UF pour y répondre.Terminologie Système : système (structure, comportement, fonction, etc.) et processus (spécification, conception, implantation, installation, opération, démantèlement, recyclage).Quatre propriétés dangereuses génériques propres aux systèmes sociotechniques concernant quatre facettes de la vie d'un système : associées à la spécification du système ; associées à la conception du système ; associées à la technologie du système ; associées à la mauvaise utilisation du système.

Partie 2 : Sécurité intrinsèque (spécification d'un système sûr)

Rappels des besoins traités et exemples d'accidents associés.Analyse des fonctions critiques : notion de criticité, utilisation d'AMDEC, etc.Modification de la spécification (prévention).Protection par redondance dont l'apport de la sécurité fonctionnelle détaillée dans l'UF 7 « Sécurité fonctionnelle ».

Partie 3 : Conception correcte (conception d'un système sûr)

Introduction : rappels des besoins de sureté de fonctionnement et exemples d'accidents associés ;Vocabulaire (faute, erreur, défaillance, propagation, latence, etc.) ; deux regards, deux approches : système et processus (conformité et correction, validation et vérification. Importance de l'homme source de fautes dans le système).Prévention des fautes : techniques applicables aux systèmes (exemple : guides de style) et aux activités humaines (exemple : processus).Détection des fautes : techniques applicables aux systèmes (exemple : test fonctionnel) et aux activités humaines (test statistique).Tolérance aux fautes : techniques applicables aux systèmes (exemple : redondance) et aux activités humaines (exemple : choix des techniques).Evaluation des fautes : introduction aux techniques d'évaluation fiabiliste développées à l'UF 6 « Sécurité structurelle » et cas de l'évaluation des fautes systémiques.Normes sectorielles : panorama des normes sectorielles (énergie -nucléaire & pétrole-, chimie, transport –avionique & ferroviaire-).Etude de cas : application spatiale

Partie 4 : Conception d'un système fiable

Le détail du cours est développé dans l'UE 6 « Sécurité structurelle ».

Partie 5 : Conception centrée utilisateur (conception d'un usage sûr)

Remarque : cette partie se focalise sur l'approche technique de la prise en compte des facteurs humains conduisant à des accidents. Les autres approches des facteurs humains ainsi que les approches liées aux facteurs organisationnels de la sécurité sont traitées dans l'UF 9 « Dimensions humaine, organisationnelle et sociale de la sécurité ».Introduction et concepts clés. Exemples d'accidents qualifiés d'erreurs humaines pour montrer ce qui renvoie à la conception pour la sécurité ; introduction des concepts d'erreurs, fautes et violations qu'elles soient humaines ou liées aux systèmes techniques ; introduction de la notion de système sociotechnique pour mettre en avant l'intérêt de prendre en compte non pas le système technique ou l'opérateur de manière isolée, mais le couplage ou la coopération Homme-Système dans un système organisé.Définition (norme ISO 13407). Connaissances générales sur le fonctionnement de l'Homme en situation. Différents types d'utilisateurs (maintenance, opérateurs, grand public, etc.). Notions de variabilité, diversité, tâches, activités, régulation. Approches de la relation homme-système (interactions et coopérations ; concepts d'utilité, utilisabilité, efficacité, efficience, acceptabilité). Caractéristiques des processus de conception : paradoxe de la spécification (degré de liberté & contraintes, projet ponctué d'irréversibilité) ; caractéristiques des problèmes de conception (problèmes mal définis, processus opportuniste, de réduction de l'incertitude, ponctué d'irréversibilités, contraint temporellement, débouchant sur des solutions acceptables) ; s'organiser pour prendre en compte les caractéristiques facteurs humains de l'utilisateur (pluralité des acteurs et conception participative) ; d'une conception technocentrée à une conception anthropocentrée.Outils et méthodes pour une conception centrée utilisateur. Méthode générale (identifier les caractéristiques et besoins des utilisateurs, analyser les tâches et activités en contexte de travail usuel, l'allocation des tâches Homme/Système, produire des solutions de conception et les matérialiser, évaluer ces solutions de façon constante).Les outils de spécification et d'évaluation : observations de situations de référence, questionnaires, entretiens, scénarii, maquettes, prototypes, simulations, brainstormings, tests utilisateurs, etc.Intégration des Facteurs Humains dans la spécification : conception participative.Normes ISO et sectorielles.Etude pratique d'analyse de conception.

Partie 6 : Robustesse à la malveillance

Cette partie sensibilise aux questions de conception de systèmes robustes à la malveillance des utilisateurs (question de « security ») et leur importance pour la sécurité (« Security for Safety »). Exemples d'accidents. Modèle d'un système automatisé (niveaux 0 à 5) et définition de ses vulnérabilités. Approches des traitements. Présentation de l'IEC 62443 incluant les 3 niveaux (Composant, Système, Politique et procédures), les concepts de « Security Lifecycle », « Security Levels » et « Maturity Levels ».

Partie 7 : Soutien Logistique Intégré

Besoins auxquels répond le Soutien Logistique Intégré, apports à la Sécurité et liens avec la Fiabilité.Présentation des processus supports (« Design for support », « Development support », et « Aquire and Provide the Support ») et du Système de Management (« Manage Logistics Support ») basé sur la norme « S-Series of ILS specifications ».

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse