

Application de la sécurité fonctionnelle conformément à la norme ISO 26262

Le problème

Avec l'avènement des systèmes d'aide à la conduite (ADAS) et de la conduite autonome, les automobiles d'aujourd'hui peuvent contenir jusqu'à 200 millions de lignes de codes (plus de 500 millions d'ici 2025) qui interagissent avec plus de 150 unités de commande. Ce nombre important d'interactions, combiné à la complexité des fonctions mises en œuvre, accroît considérablement les préoccupations liées à la sécurité. C'est pour répondre à ces préoccupations que la norme ISO 26262 a été élaborée pour l'industrie automobile. En effet, cette norme définit un cadre de développement fondé sur certaines exigences en matière de sécurité.

Cette norme décrit de nouvelles méthodes pour le développement, la validation et la vérification des systèmes logiciels utilisés par l'industrie automobile. Les fabricants de systèmes et de sous-systèmes devront faire appel à des intervenants externes pour pouvoir utiliser ces nouvelles plateformes rapidement et efficacement.

Produits et services

CS Canada possède le savoir-faire requis pour développer, valider et vérifier des systèmes et des logiciels, et pour embarquer des systèmes critiques sur le plan de la sécurité conformément à la norme ISO 26262.

- Conception de la sécurité fonctionnelle – ISO 26262 Partie 3
 - Déterminer les dangers, évaluer les risques et analyser les niveaux d'intégrité de sécurité automobile (ASIL)
 - Élaborer le concept de sécurité fonctionnelle
 - Déterminer les exigences de sécurité fonctionnelle
- Développement du produit au niveau du système – ISO 26262 Partie 4
 - Passer du concept de sécurité fonctionnelle au concept de sécurité technique plus précis
 - Valider la sécurité
 - Déterminer les exigences de sécurité technique
- Développement du produit au niveau du logiciel – ISO 26262 Partie 6
 - Spécifier, concevoir, mettre en œuvre et vérifier rigoureusement le logiciel embarqué en temps réel
 - Effectuer une répartition spatiale et temporelle (absence d'inférence)
 - Déterminer les exigences de sécurité logicielle

- Planification et gestion efficaces des activités de sécurité – ISO 26262 Partie 2
 - Définir les rôles requis en lien avec la sécurité au sein de l'organisation (gestionnaires et ingénieurs de sécurité)
 - Définir clairement les responsabilités et communiquer pendant la durée du cycle de vie
 - Développer le Plan de Sûreté
- Établir les processus de soutien nécessaires - ISO 26262 Partie 8
 - Outils de gestion du changement et de la configuration
 - Élaboration d'un plan de vérification et automatisation des tâches de vérification
 - Qualification et utilisation d'outils qualifiés
- Adaptation de méthodes et techniques éprouvées à partir de la vérification de logiciels critiques du secteur aérospatial afin de les utiliser dans le développement de systèmes automobiles à niveau d'intégrité de sécurité très élevé (ASIL)
 - Communiquer avec les autorités chargées de la sécurité et appliquer des moyens efficaces de se conformer
 - Mettre en place une structure organisationnelle afin de garantir l'indépendance
 - Faire le suivi des exigences et justifier les mesures de sécurité (ARP-4754A)

Avantages

Grâce à notre soutien, nos clients de l'industrie automobile peuvent mettre en œuvre la norme ISO 26262 rapidement et efficacement, et ainsi garantir la sécurité de leurs systèmes et des gens à l'intérieur et à proximité de leurs automobiles.

Pourquoi faire affaire avec CS Canada?

Afin de pouvoir relever les défis liés à la norme ISO 26262, CS Canada a mis sur pied une équipe hautement qualifiée possédant une vaste expérience dans le développement, la vérification et la validation de logiciels temps réel critiques. Réalisations de notre équipe :

- Depuis plus de 7 ans, nous mettons notre expertise en matière de systèmes et de sécurité au service de l'industrie automobile afin de développer des fonctions d'aide à la conduite automobile évoluées
- Adaptation de méthodes et techniques éprouvées à partir de la vérification de logiciels critiques du secteur aérospatial afin de les utiliser dans le développement de systèmes automobiles à niveau d'intégrité de sécurité très élevé (ASIL)
- Utilisation de méthodes et d'outils avancés (p. ex. les méthodes formelles) pour relever les défis liés aux logiciels de plus en plus complexes pour les automobiles
- Vaste expérience reposant sur la certification DO-178 de plus de 30 programmes aéronautiques