J3061 Cybersécurité pour les systèmes de véhicules cyber-physiques

Le problème

Grâce aux progrès technologiques liés aux systèmes d'aide à la conduite et aux véhicules autonomes, les automobiles peuvent interagir avec un nombre infini de systèmes et de réseaux. Ces interactions passent par différents protocoles de communication (Bluetooth, CAN, OBD-II, ethernet et autres) et peuvent constituer des menaces sérieuses à la cybersécurité.

Nous savons déjà que le protocole CAN comporte des failles de sécurité, car il n'est doté d'aucune procédure de chiffrement ou d'authentification par défaut. Pour ce qui est des codes source, une automobile peut maintenir contenir jusqu'à 200 millions de lignes de codes (plus de 500 millions d'ici 2025). Ces codes peuvent comprendre des failles de sécurité pouvant être directement exploitées. Il existe beaucoup d'autres vecteurs d'attaque, comme les réseaux sans fil et les fichiers exécutables malveillants. Les bulletins de nouvelles ont rapporté des attaques aux freins et au moteur du Jeep Cherokee (2015) et à l'application de contrôle à distance du Nissan Leaf (2015), la vulnérabilité du système de déverrouillage à distance de nombreux fabricants (2015) et la désactivation des freins à distance du Tesla Model S (2016).

Avec toutes ces attaques et vulnérabilités potentielles, la cybersécurité est une discipline qui ne peut être ignorée et qui doit être intégrée dès les premières étapes de votre processus de développement de système.

Produits et services

CS Canada possède le savoir-faire requis pour effectuer l'évaluation complète de la sécurité et la mise en œuvre du processus de sécurité des systèmes critiques sur le plan de la sécurité conformément à la norme J3061. Nous vous offrons les services suivants :

- Application des principes de conception sûre
  - Application judicieuse des mesures de sécurité à l'architecture de système
  - Recommandation des meilleures pratiques concernant les mesures de sécurité pour l'authentification et le chiffrement
  - Détermination des lacunes dans l'architecture de sécurité
- Élaboration du dossier de cybersécurité
  - Analyse de la conformité aux exigences de sécurité
  - Examen des questions de sécurité en suspens

1-866-748-8258
info@cscanada.ca
www.cscanada.ca

Montréal (Québec), Canada
East Hartford, CT, USA

  - Preuves et arguments démontrant que le système comporte le niveau de sécurité prévu à l'étape de la conception initiale
  - Plan d'action pour régler les questions de sécurité en suspens
- Détermination des objectifs de sécurité et exécution de l'analyse des menaces et de l'évaluation des risques (TARA)
- Compréhension de la façon de produire de la documentation répondant aux critères pour la certification
- Examen des codes conformément à la norme de codage sécuritaire CERT C à l'aide d'outils d'analyse des codes comme LDRA
- Expertise requise pour aider les clients du secteur automobile à élaborer des approches sur mesure pour se conformer aux normes ISO 26262 et SAE J3061 et offre de conseils et de connaissances supplémentaires s'appuyant sur l'expérience dans le secteur aérospatial et dans d'autres domaines techniques

Avantages

Grâce à notre soutien, nos clients de l'industrie automobile peuvent mettre en œuvre la norme J3061 rapidement et efficacement, et ainsi garantir la sécurité de leurs systèmes et des gens à bord et à proximité de leurs véhicules.

Pourquoi faire affaire avec CS Canada?

Afin de relever les défis liés à la cybersécurité, CS Canada a mis sur pied une équipe hautement qualifiée et très expérimentée dans le développement, la vérification et la validation de logiciels temps réel critiques. Réalisations de notre équipe :

- Plusieurs accréditations de sécurité : Certifications Systems Security Practitioner d'ISC2, Security Essentials de l'ACEG, membre du conseil consultatif de l'ACEG, certification Information Systems Auditor d'ISACA
- Expérience dans l'évaluation de la sécurité dans les secteurs aérospatial, ferroviaire et automobile - Membre du Comité spécial de la RTCA qui a rédigé les trois normes de sécurité DO de la RTCA
- Vaste expérience dans l'utilisation d'outils d'analyse statiques et dynamiques pour détecter les failles de sécurité du code source dans de nombreuses industries