Cybersécurité du véhicule connecté

1 jour (7 heures)

Tarif inter : de 700 € HT à 750 € HT
Tarif intra : nous consulter

FORMATION EN PRESENTIEL

Dates, lieux et tarifs sur sia.fr

Personnel concerné

Toute personne de la filière automobile impliquée dans la conception, la fabrication ou la commercialisation de systèmes embarqués intégrant des fonctionnalités à base de composants électriques, électroniques ou logiciels.

Prérequis

Avoir une connaissance basique du fonctionnement d'un véhicule automobile et des principes de l'électronique.

Animateur

Yacine LADJICI, Group Cybersecurity Officer de Valeo, Président du groupe de travail « Cybersécurité » du Comité de Standardisation Technique Automobile de la PFA.

Méthodes et moyens pédagogiques

Apports théoriques avec support Powerpoint
Séquences de questions/réponses afin de favoriser l'interactivité.
Remise d'un support de cours au format électronique.

Moyens techniques

Salle de formation climatisée, équipée d'un vidéoprojecteur, d'un écran et d'un paper board.

Suivi et évaluation

Feuille d'émargement signée par demi-journée par les stagiaires et cosignée par le formateur.
Évaluation de la formation par les participants.
Évaluation des acquis par l'intermédiaire d'un QCM effectué en fin de formation.
Remise d'une attestation de formation.

Délais d'accès

Inter-entreprises : inscription au plus tard 2 jours avant la formation
Intra-entreprise : organisation sous deux semaines minimum.

Accessibilité aux personnes en situation de handicap

Contacter notre référent handicap : referenthandicap@sia.fr

OBJECTIFS

Être capable :

- D'identifier les différentes fonctions du véhicule impactées par la cybersécurité,
- De décrire la structure d'une architecture électrique et électronique d'un véhicule,
- De citer les protocoles de communication véhicule et leur lien avec la cybersécurité,
- De décrire les différents types d'architecture (véhicules, navettes),
- D'identifier les grandes familles d'attaques contre le véhicule connecté,
- De faire la différence entre une attaque embarquée et une attaque débarquée.

PROGRAMME

Introduction et contexte

- Les grands types de menace cyber
- Les motivations des attaquants
- Les attaques actuelles de l'industrie automobile.

L'architecture électrique/ électronique

- Les fonctions du véhicule et les systèmes associés
- Les inducteurs et les technologies
- Les protocoles de communication : CAN/LIN/Ethernet/FlexRay
- Les spécificités des architectures de navettes automatisées.

Les standards structurants d'une architecture électrique/ électronique

- Découverte de l'ISO 26262
- Découverte de l'ISO/SAE 21434
- Mise en pratique de la norme cyber
- Le V2X
- La réglementation cyber dans l'automobile UN-R 155
- L'annexe 5 de l'UN-R 155.

Les menaces cyber et les mesures d'atténuation externes

- Attaques contre les serveurs débarqués
- Attaques avec brèche de données
- Attaques par opérateurs internes ou externes.

Les menaces cyber et les mesures d'atténuation internes

- Attaques par le biais des interfaces physiques
- Attaques adjacentes
- Attaques réseau
- Attaques par spoofing
- Attaques replay et relay
- Attaques V2X.

Conclusion

Contact : Larissa RIFFAUD
larissa.riffaud@sia.fr // 07 86 76 12 79

MAJ 11-12-2023