Communiqué de presse

FEV France : Z.A. de Trappes – Élancourt, 11 rue Denis Papin, CS 70533 – Trappes, 78197 Saint Quentin en Yvelines Cedex

Création par FEV d'une plateforme répondant aux risques liés à la cybersécurité sur les nouveaux véhicules

Aix-La-Chapelle, 25.05.2021 - FEV, l'un des principaux fournisseurs de services mondiaux de développement de matériel et de logiciels pour les véhicules et les groupes motopropulseurs, a constaté que l'utilisation croissante de logiciels dans les véhicules représentait un risque de sécurité informatique important. Pour y répondre, FEV a créé une nouvelle plateforme méthodologique, appelée SPORT (Stratégie, Process, Organisation, Ressources et Technologie), qui permet aux constructeurs et aux équipementiers d'agir rapidement et de garder une longueur d'avance sur les hackers.

La plateforme de FEV est conçue pour fournir une approche globale de la cybersécurité. La partie **Stratégie** prend en compte la vision, la mission et la culture d'entreprise du constructeur ou du fournisseur. Cette étape permet d'aligner la stratégie de cybersécurité sur la stratégie de l'entreprise et décrit son impact sur le portefeuille de produits actuel et futur ainsi que sur celui des clients.

L'étape **Process** intègre des phases de développement, par exemple le SDLC (Security Development Life Cycle), la gestion des connaissances, ainsi que des sessions d'audit et de formation, soutenue par des actions dédiées pour accompagner cette évolution.

L'Organisation permet de définir la structure des équipes de cybersécurité et développe une structure de reporting avec des rôles et des responsabilités clairs, tandis que la partie **Ressources** définit la taille de l'équipe nécessaire et s'occupe des stratégies d'acquisition de talents et d'externalisation.

Enfin, l'étape **Technologie** intègre :

- Une stratégie matérielle et logicielle hautement sécurisée
- Des mesures techniques
- Les outils et l’infrastructure disponibles

Le développement de l'industrie automobile et l’intégration croissante des technologies de l'information dans les véhicules font de la plateforme de FEV un service précieux pour les constructeurs automobiles : en 2010, une voiture haut de gamme comptait jusqu'à 100 millions de lignes de code logiciel, aujourd'hui elle est proche de 150 millions de lignes. D'ici 2030, le nombre devrait être supérieur à 300 millions. Cette augmentation de la taille des programmes offre beaucoup plus de points d'entrée pour les cybers attaques.

Ces dernières années, l'importance de la cybersécurité a déjà eu un impact sur les résultats financiers de grands acteurs des secteurs de l'automobile et de la technologie. Une poignée d'attaques très médiatisées a directement entraîné une baisse du cours des actions, ainsi qu'une atteinte aux performances et à la réputation de nombreuses entreprises. À titre d'exemple, une attaque à distance en 2015 a entraîné le rappel de près de 1,5 million de véhicules. Cela a conduit à des coûts estimés à 600 millions de dollars et à une perte estimée de 4 milliards de dollars en bourse pour ce constructeur.

Avec la complexité croissante des véhicules, il est probable que ces événements deviendront encore plus courants. De plus en plus d'informations sur les conducteurs seront sauvegardées et accessibles via le véhicule, augmentant ainsi les risques de futures attaques.

« *La cybersécurité continuera de jouer un rôle de plus en plus important pour les constructeurs automobiles mondiaux dans les années à venir, à mesure que les véhicules deviendront de plus en plus connectés et automatisés* », a déclaré Mayank Agochiya, directeur général de FEV Consulting, Inc.

Outre une diminution de leurs pertes financières, les mesures de cybersécurité offrent également aux constructeurs l’opportunité de se différencier. Étant donné que les propriétaires et les utilisateurs de véhicules se voient offrir des fonctionnalités de connectivité hautement intégrées, la confiance jouera un rôle important dans leur acceptation.

Compte tenu de ces facteurs, l'industrie de la mobilité accorde une plus grande attention à la cybersécurité. La conformité à la majorité des réglementations et des normes de cybersécurité, y compris la norme ISO 21434, est attendue pour les véhicules commercialisés dès 2025. Avec la mise en place du WP.29 de la CEE, la cybersécurité deviendra un aspect obligatoire de l'homologation dans 54 pays avant même 2025. Pour être en conformité, les équipementiers et les fournisseurs doivent agir dès maintenant. Des organisations, des ressources et des processus de cybersécurité complexes doivent être mis en place et prêts d'ici la fin de 2022.

« *Une action rapide et proactive est nécessaire pour que les constructeurs et les fournisseurs soient prêts d'ici 2025 au plus tard* », a déclaré Agochiya, « *Grâce à notre méthodologie SPORT, nous sommes fiers d'offrir à nos clients un soutien dans leur quête de développement de véhicules plus sûrs*. »

La méthodologie de FEV a déjà réussi à identifier et à réduire les risques en agissant tôt et en utilisant une approche appropriée. Elle a démontré que les équipementiers et les fournisseurs du secteur de la mobilité peuvent à la fois protéger leurs finances contre les risques de cyber attaques et améliorer la sécurité des passagers.

Pour en savoir plus : https://www.fev-consulting.com/en.html

À propos de FEV

FEV est l'un des principaux fournisseurs indépendants de services internationaux dans le développement de véhicules et de groupes motopropulseurs pour le matériel et les logiciels. L'expertise de FEV s'étend du conseil au développement et aux essais de concepts de véhicules innovants jusqu'à leur production en série. En complément du développement des chaines de traction traditionnelles, de l'intégration des véhicules, de la calibration et de l'homologation des nouveaux moteurs essence et diesel, une importance croissante est accordée au développement des groupes motopropulseurs hybrides et électriques ainsi que des carburants de remplacement. Les experts de FEV se concentrent sur le développement des systèmes de contrôle électronique, ainsi que sur les véhicules autonomes et connectés. Les activités d'électrification des groupes motopropulseurs couvrent les puissants systèmes de batteries, les machines électroniques et les onduleurs. En outre, FEV développe des moteurs à essence et diesel très efficaces, des groupes moto-propulseurs complets ainsi que des systèmes de piles à combustible et facilite leur intégration dans les véhicules adaptés à l'homologation. Les carburants alternatifs sont un autre domaine de développement.

Le portefeuille de services sur mesure est complété par des bancs d'essais et une technologie de mesure, ainsi que par des solutions logicielles qui permettent un transfert efficace des étapes de développement essentielles, de la route au banc d'essai ou à la simulation.

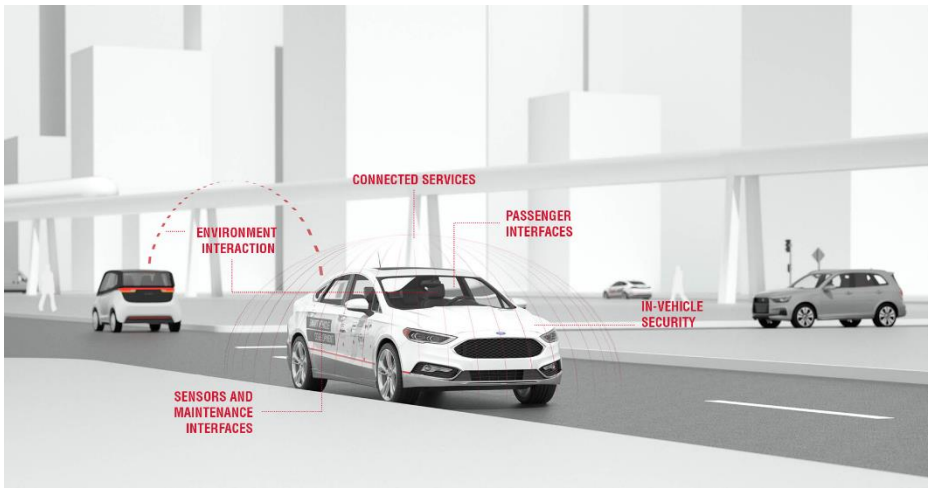
Le Groupe FEV emploie plus de 6300 spécialistes hautement qualifiés dans des centres de développement modernes à proximité de ses clients sur plus de 40 sites répartis sur quatre continents.

A propos de FEV France

Avec plus de 750 collaborateurs en France, FEV offre son expertise d'ingénierie, ses services et ses équipements, au développement des groupes motopropulseurs innovants qu'ils soient thermiques, hybrides ou électriques. La société propose des solutions à la pointe de la technologie, toujours plus respectueuses de l'environnement avec un haut niveau d'exigence en termes de qualité, de respect des délais, de sécurité, de performances et de fiabilité. FEV est également le partenaire privilégié des acteurs majeurs de l'industrie du transport français : constructeurs, équipementiers, laboratoires d'essais, écoles et universités.

Galerie photos

[FEV – Cybersécurité] – Source : FEV Group



SPORT de FEV est conçu pour fournir une vue globale de cybersécurité. Il est prouvé qu'en agissant tôt et en utilisant une approche appropriée, les équipementiers et les fournisseurs peuvent protéger leurs finances contre le risque de cyberattaques et améliorer la sécurité des passagers.