Fiche d'information

Si c'est la fin de l'OBD-II, qu'est-ce qui le remplacera?

Certains prédisent la fin prochaine de l'OBD-II

L' actuelle interface de communication avec le véhicule (ICV) — le port de diagnostic embarqué (OBD) sous le tableau de bord – est dépassée. Bien que les utilisateurs puissent facilement accéder aux données, logiciels et autres informations d'un véhicule en branchant un analyseur-contrôleur ou un autre dispositif de diagnostic, l'industrie s'entend que l'architecture actuelle et ses protocoles ne répondent plus aux besoins contemporains.

Source: Telematics Talk (en anglais seulement)

On voit déjà certaines indications que les constructeurs de véhicules désirent restreindre l'accès au système OBD-II (dans certains cas, ils ont rendu physiquement difficile de garder un dispositif de type clé électronique branché dans le port lorsqu'un véhicule fonctionne).

Source: MAPSA (en anglais seulement)

Deux nouvelles interfaces de communication de véhicule en lice pour remplacer le système OBD-II

Interface de véhicule sécurisée (IVS)

Exige que le module passerelle soit installé à l'intérieur du véhicule et qu'il utilise des protocoles de sécurité pour gérer l'accès, soit au moyen du port actuel situé sous le tableau de bord (non recommandé par la SAE), d'un nouveau port d'accès ou de communications sans fil.

Source: Telematics Talk (en anglais seulement)

Véhicule étendu

Exige que, lors de l'accès initial, les mesures de sécurité de la passerelle soient à l'extérieur du véhicule, dans le serveur infonuagique du constructeur de véhicules.

Source: Telematics Talk (en anglais seulement)

La sécurité par l'obscurité

Il semblerait logique d'affirmer que l'interface ouverte IVS est la moins sécurisée des deux. L'expression « la sécurité par l'obscurité » sert souvent à décrire comment les interfaces fermées réalisent la sécurité. Fait intéressant, on soutient plutôt que les interfaces ouvertes sont plus sécurisées en raison – justement – de leur ouverture.

Ce principe de conception ouverte est partagé par le département de la Défense (DoD) des États-Unis. Selon le DoD, la conception ouverte facilite l'identification et la correction de failles de sécurité pour des tierces parties comme les propriétaires ou les fabricants du marché secondaire du secteur des parcs de véhicules. À l'opposé, un système fermé dépend d'une équipe restreinte de développement pour déceler et corriger les problèmes. Le passé a démontré que ces équipes centralisées sont souvent dépassées par les menaces à la sécurité. C'est pourquoi, d'après le DoD, « la sécurité par l'obscurité » est généralement dénigrée.

Source: Geotab (en anglais seulement)

Restez à l'affût pour obtenir plus de renseignements et savoir comment participer à la conversation sur l'accès aux données du véhicule.

Association des industries de l'automobile du Canada
180 rue Elgin, Bureau 1400 | Ottawa, Ontario K2P 2K3 | Tél : (800) 808-2920 | Téléc : (613) 728-6021 | info@aiacanada.com