Le sfide nell'Automotive Cybersecurity per la Conformità a UNECE WP.29 UN-R 155 e ISO/SAE 21434

14 marzo 2023 ore 10:00

WEBINAR

14 marzo 2023

Ore 10:00 – 11:00

Con l'introduzione del regolamento UNECE WP.29 **UN-R 155,** nuovi **requisiti** sono stati aggiunti alle **certificazioni** dei nuovi modelli di **veicoli**. **OEM, fornitori, test-house ed enti di certificazione** si stanno confrontando con le sfide collegate a queste novità.

Keysight ha lavorato a lungo con le parti interessate del settore automobilistico sul fronte dei **test** per la robustezza della **cybersecurity** dei prodotti (**veicolo, sottosistemi, ECU/TCU**), grazie alla propria esperienza decennale nell'ambito dei test funzionali e di sicurezza informatica di interfacce cablate e wireless, ottenuta anche tramite l'acquisizione di Ixia nel 2017.

In questo ambito, Keysight supporta i clienti con apposite piattaforme di test per Automotive Cybersecurity per permette alle aziende di **collegare** i propri **requisiti**, i risultati del **TARA** (Threat Analysis and Risk Assessment) ed i **test**. Per mantenere basso il livello delle minacce, è essenziale, infatti, disporre di tutte le informazioni in un'unica postazione, ed è quindi necessario implementare ed utilizzare un CSMS (Cyber Security Management System) in accordo allo standard **ISO/SAE 21434**.

Durante il webinar verranno presentati i fondamenti per affrontare le problematiche di Automotive Cybersecurity, quali rischi vi sono per i nuovi veicoli, quali standard e regolamenti sono in vigore, perché è importante adottare un CSMS, quali processi e soluzioni sono necessari per sviluppare, produrre e omologare veicoli e componenti.

A chi è dedicato questo webinar?

Chief Information Officer, Chief Information Security Officer, Operation Manager, Project and Production Manager, Quality Manager, Auditor, Cybersecurity Manager, Product Engineer, Sviluppatori, Testing Engineer.

Giancarlo Albiero
Responsabile Marketing, Aftermaket e Motorsport ANFIA

Davide Di Marzio
Account Manager Keysight Technologies

Eliana Rossi
Wireless Automotive Solutions Architect Keysight Technologies

Davide Buccheri
Software and Automotive Cyber Security Engineer Reinova

AGENDA

10.00 **Benvenuto e Introduzione**

a cura di Giancarlo Albiero – ANFIA
Davide Di Marzio – Keysight Technologies

- Cosa accade ai nostri veicoli in strada
- Perché accade – un'analisi delle cause principali

Regolamenti e Best Practice: come orientarsi

a cura di Eliana Rossi – Keysight Technologies

- UN-R 155 e ISO/SAE 21434 – un confronto
- Requisiti per Essere Compliant: Security System e Product Development
- Automotive Cybersecurity Lifecycle e Workflow

Reinova: overview della Testing Facility e attività
a cura di Davide Buccheri – Reinova

- CANBus, Connettività di Bordo e Test Analysis

Tool e Soluzioni per affrontare le nuove sfide
a cura di Eliana Rossi

10.45 **Q&A**
Davide Buccheri – Reinova
Eliana Rossi & Thomas Leifert, Keysight Technologies

11.00 **Wrap-up**
Giancarlo Albiero – ANFIA
Davide Di Marzio, Keysight Technologies

Iscrizioni

La **partecipazione** è **gratuita** previa registrazione.
Il giorno precedente il webinar saranno inviate le credenziali per accesso alla piattaforma.

Il Contesto

La guida autonoma, le auto connesse, i veicoli elettrici e la mobilità condivisa hanno dominato l'agenda dei leader dell'industria automobilistica negli ultimi anni.
Queste **innovazioni**, basate sulla **digitalizzazione dei sistemi di bordo**, l'estensione dei **sistemi IT dei veicoli nel back-end**, l'aumento delle **interfacce di comunicazione cablate e wireless**, trasformano le auto moderne in clearinghouse delle informazioni, rendendole anche **bersagli allettanti per gli attacchi informatici**.
Le case automobilistiche hanno acquisito consapevolezza dell'impatto che un attacco informatico può avere sui veicoli dei loro marchi, causando danni sia alla sicurezza dei passeggeri che alla reputazione del marchio stesso.

In questo contesto, sia i legislatori che gli organismi di regolamentazione per la sicurezza e gli esperti dell'industria automobilistica, hanno sviluppato regole comuni per la gestione della sicurezza informatica nel settore automobilistico. **ISO/SAE 21434, UNECE WP.29, regolamento R155, CSMS (Cyber Security Management System)** sono alcune delle parole chiave da conoscere. È fondamentale gestirne adeguatamente le implicazioni formali, soprattutto a partire da luglio 2022 per l'applicazione del nuovo Regolamento UE. **Nuovi Regolamenti e Standard** rendono la **sicurezza informatica automobilistica** non negoziabile per garantire l'accesso al mercato e l'omologazione **negli oltre 60 paesi membri UNECE WP.29 o dell'Unione Europea**.

Pertanto, gli **OEM, i fornitori, le test-house** e gli **enti di certificazione** devono comprendere i requisiti che sono stati aggiunti alle nuove certificazioni dei veicoli dal **Regolamento R155**, quali **sfide** queste parti interessate hanno **osservato e discusso con Keysight**, e quali **strumenti** e **soluzioni** sono stati sviluppati grazie al collaborazione con clienti e partner come Reinova.

Per implementare correttamente il CSMS secondo ISO/SAE 21434 e mantenere basso il livello di minaccia:
- Sul fronte dello **sviluppo del prodotto**, è necessaria una piattaforma di test con più interfacce HW, scalabile e con software aggiornato costantemente, che consenta di **validare la robustezza** dell'intero **veicolo**, dei suoi sottocomponenti e delle ECU/TCU rispetto agli attacchi informatici in continua evoluzione.
- Sul fronte della **sicurezza aziendale** e della conformità dei sistemi IT di back-end**, è essenziale** collegare i requisiti**, i risultati dell'analisi delle minacce e della** valutazione dei rischi **(TARA - Threat Analysis and Risk Assessment)** ed i test, attraverso un'unica piattaforma che raccolga tutti i dati.