aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

CYBERSECURITY IN EUROPA

Roma, 11 APRILE 2024

Automotive e cybersecurity: vulnerabilità, sistemi di protezione e quadro normativo

Massimo Centofanti

Cybersecurity Division Director

Mi presento

Massimo Centofanti

Cyber Sec Division Director @aizoOn

Ethical Hacker, CISO, IT Security Consultant, oltre che DPO in realtà della PA e Private, opero quale Cyber Security Division Director in una realtà multinazionale consolidata nel mercato delle soluzioni e dei servizi di Sicurezza. Sono stato responsabile presso i Security Operation Center di diverse infrastrutture critiche del settore Oil & Gas e altri settori industriali. Sono un membro permanente del tavolo dedicato alla cyber security della Camera di Commercio Americana, partecipo attivamente al gruppo di lavoro sulla cyber security di ANFIA - Associazione Italiana dell'Industria Automotive, sono inoltre membro di diverse community di ricercatori di sicurezza

Premessa

L'Automotive Cyber Security è la sfida del momento per le case automobilistiche. **Ogni interfaccia di comunicazione potrebbe rappresentare un potenziale punto di attacco per i criminali informatici**. Il potenziale di danno della manipolazione sta aumentando rapidamente, per esempio per quanto riguarda i veicoli a controllo autonomo o le funzioni di guida e di frenata controllate elettronicamente.

Per questo motivo, le Nazioni Unite hanno definito il quadro di base per la sicurezza informatica automobilistica con due nuovi regolamenti. Questi sono **UNECE Cyber Security (UN R 155), che si riferisce direttamente al nuovo standard ISO/SAE 21434, e UNECE Software Updating (UN R 156).** Nel luglio 2022 sono entrate in vigore le norme per i nuovi tipi di veicoli (nell'UE). **L'industria automobilistica sta quindi affrontando grandi sfide** - soprattutto perché molti produttori di apparecchiature originali (OEM) e fornitori criticano i nuovi regolamenti come molto generici. **Vi è un desiderio diffuso di raccomandazioni concrete.**

Ma sono “hackerabili” le automobili?

Il Global Automotive Cybersecurity Report 2024 di Upstream segnala **oltre 1.468 incidenti informatici legati a veicoli connessi** dal 2010, con la preoccupazione che il fenomeno possa crescere considerevolmente nei prossimi anni.

Dal 2023 si è verificato un aumento degli incidenti e degli attacchi informatici che interessano molti veicoli connessi. **Il 50% di questi incidenti ha avuto un impatto significativo** sul veicolo e sul conducente, e **il 95% degli attacchi è stato condotto a distanza**.

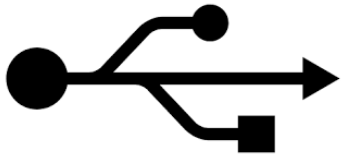
Ma sono “hackerabili” le automobili?

Attacchi Wireless

Keyless Entry Hack: Gli attaccanti possono utilizzare dispositivi per estendere il segnale dalla chiave intelligente del veicolo, **permette**ndo loro **di sbloccare e avviare l'auto da una distanza significativa**, un metodo noto come "relay attack".

Attacchi via Bluetooth o Wi-Fi: Sfruttando vulnerabilità nei sistemi Bluetooth o Wi-Fi del veicolo, gli hacker possono guadagnare accesso per manipolare varie funzioni o rubare dati personali.

OBD II



Attacchi su Interfacce Fisiche

OBD-II Hacking: La porta diagnostica OBD-II, che fornisce accesso ai dati del veicolo e al controllo su alcuni sistemi, può essere sfruttata per iniettare codice malevolo o manipolare le funzionalità dell'auto.

Attacchi tramite USB: Dispositivi USB malevoli possono essere utilizzati per installare malware o compromettere i sistemi di bordo quando connessi all'interfaccia multimediale dell'auto.

Ma sono “hackerabili” le automobili?

Attacchi ai Sistemi di Infotainment

Infiltrazione via Infotainment: Sfruttando le vulnerabilità **nei sistemi di infotainment, gli attaccanti possono installare malware o guadagnare accesso** a reti più critiche all'interno del veicolo.

Manomissione dei Media: Inserendo media infetti (come SD card o dispositivi USB), gli aggressori possono **compromettere il sistema di infotainment per eseguire codice arbitrario**.

Manomissione dei Sistemi di Navigazione e Telematica

Spoofing GPS: Gli attaccanti possono **inviare segnali GPS falsi** per ingannare il sistema di navigazione del veicolo, **potenzialmente deviando il percorso**.

Compromissione dei Dati Telematici: Interferendo **con i dati trasmessi dai sistemi telematici**, gli hacker **possono intercettare informazioni sensibili o inviare comandi falsi al veicolo.**

Ma sono “hackerabili” le automobili?

Attacchi alla Rete di Bordo (CAN Bus)

Iniezione di Frame CAN: Gli attaccanti possono **inserire o modificare i frame sul bus CAN**, che è il sistema di comunicazione principale tra i moduli elettronici del veicolo, **per controllare le funzioni del veicolo** o generare malfunzionamenti.

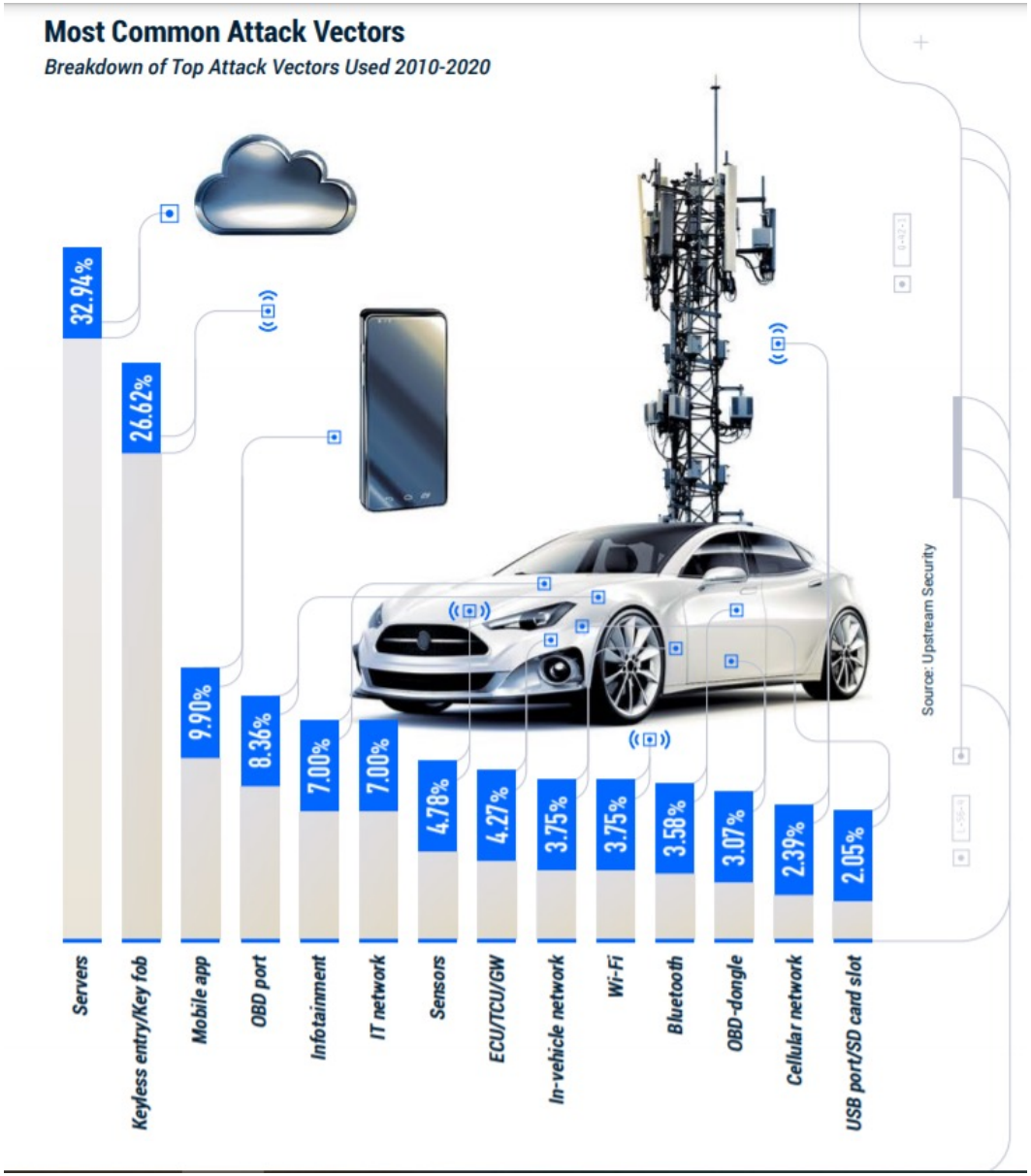
Attacchi alle Funzionalità di Guida Autonoma e Assistenza alla Guida

Interferenza con i Sensori: Gli attacchi possono **mirare ai sensori (LIDAR, radar, telecamere)** dei sistemi di assistenza alla guida, **causando la lettura di dati falsi e potenzialmente provocando comportamenti pericolosi**.

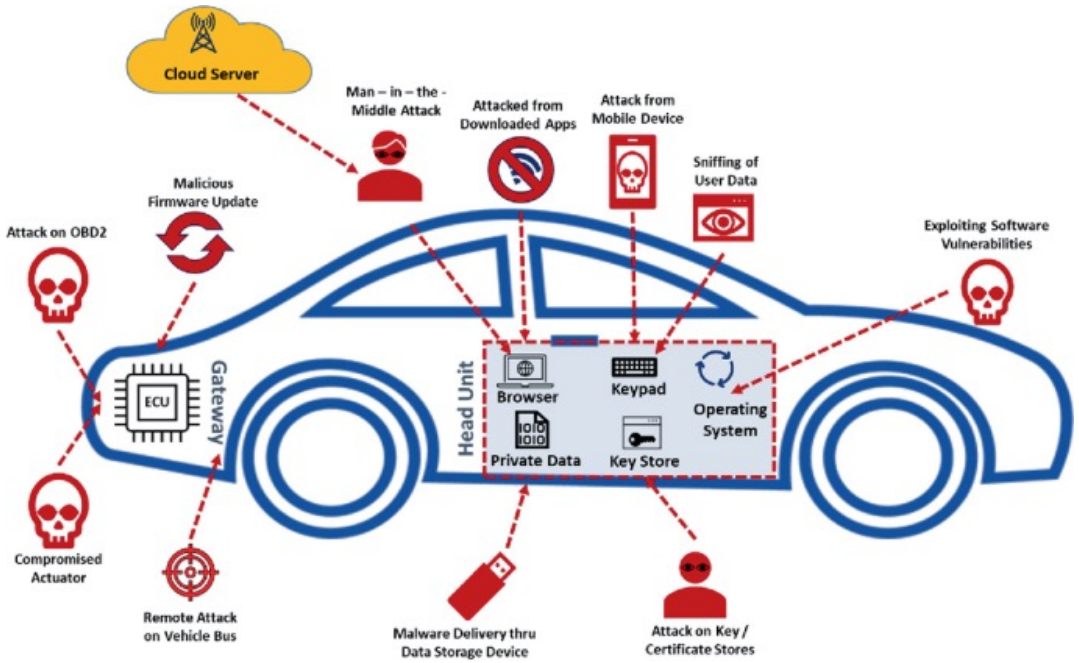
Manipolazione del Software di Guida Autonoma: Compromettendo il software di guida autonoma, **gli hacker potrebbero prendere il controllo delle funzioni di guida** del veicolo.

Scenario

Veicoli connessi: questo significa sistemi di assistenza innovativi, guida (parzialmente) autonoma, produzione in rete con i fornitori, auto connesse con servizi connessi - **la digitalizzazione si sta facendo sentire chiaramente in quasi tutti i settori dell'industria automobilistica**, e sta progredendo rapidamente. Ma **la crescente connettività significa in definitiva sempre più codici, e quei codici possono essere compromessi in molti modi**. Dopo tutto, le auto moderne contengono fino a 150 unità di controllo elettronico e circa 100 milioni di linee di codice, che si prevede di triplicare entro il 2030. **La quantità di software nei veicoli di oggi è già quattro volte quella di un jet da combattimento.**



Scenario



Non è solo dopo la pandemia e il relativo aumento degli attacchi informatici che si deve prestare particolare attenzione alla sicurezza informatica o alla sicurezza informatica automobilistica. Un veicolo deve essere in grado di garantire la sua sicurezza funzionale in ogni momento. **Il potenziale di danno degli attacchi informatici alle auto intelligenti è enorme**. Devono essere considerati gli scenari drammatici di attacchi su larga scala ("**Tutti i freni elettronici dei veicoli di un produttore vengono paralizzati simultaneamente da un attacco hacker**"). Occorrono quindi concetti di sicurezza accurati ed efficaci.

Scenario

Oggi, le misure selettive non sono più sufficienti per proteggere i veicoli in modo olistico. Invece, **sono necessari approcci sistematici e strategici che specificano requisiti chiari per la portata, le prestazioni e la verifica di un sistema di sicurezza**. L'approccio strategico dovrebbe coprire l'intero ciclo di vita del prodotto. Qui, l'attenzione deve concentrarsi sulla disponibilità a lungo termine degli aggiornamenti del software, per esempio, o sull'integrazione dell'intera supply chain.

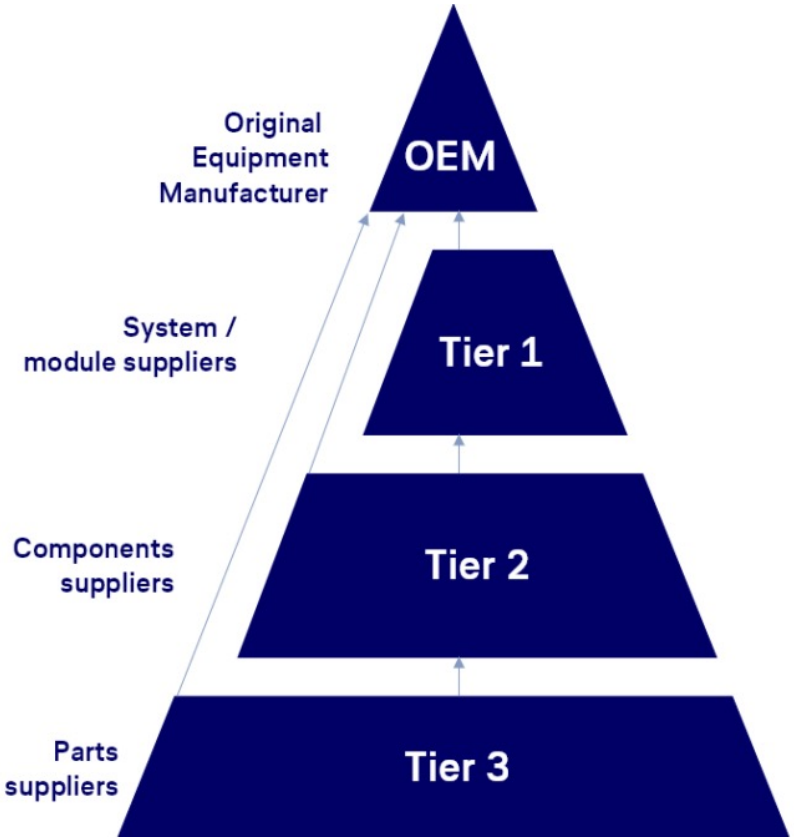
I regolamenti: UNECE R155 e R156

I regolamenti sono entrati in vigore all'inizio del 2021. **Da luglio 2022, la conformità è obbligatoria per i nuovi tipi di veicoli**. I costruttori che non soddisfano i requisiti dovranno poi affrontare la non immatricolazione dei relativi tipi di veicoli. Infine, **da luglio 2024, i regolamenti si applicheranno a tutti i veicoli di nuova fabbricazione.**

I regolamenti richiedono essenzialmente l'attuazione di misure in quattro aree:

- **Gestione dei rischi informatici per i veicoli**
- **Protezione dei veicoli secondo un approccio security-by-design per mitigare i rischi lungo la catena del valore**
- **Rilevamento e difesa dagli attacchi su tutta la flotta di veicoli**
- **Fornitura di aggiornamenti software in termini di sicurezza e introduzione di una base legale per gli aggiornamenti over-the-air (O.T.A.) del software del veicolo**

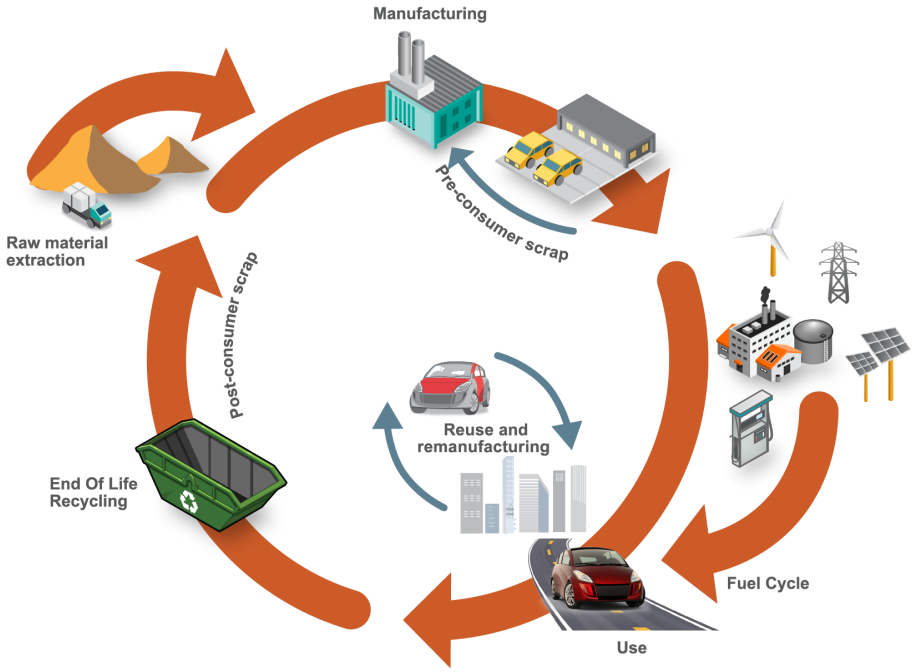
I regolamenti si applicano…



I regolamenti dell'ONU parlano **principalmente di produttori di veicoli** che devono implementare i nuovi requisiti. Tuttavia, questo include il monitoraggio e la verifica della sicurezza informatica in tutta la catena di fornitura per dimostrare l'applicazione dei regolamenti in ogni momento. **Il produttore è quindi obbligato a monitorare i fornitori**. E quindi molto probabilmente richiederà anche ai suoi fornitori di implementare i nuovi standard.

I due regolamenti si applicano **alle autovetture, furgoni, camion e autobus**, a condizione che siano dotati di funzioni di guida automatizzata. Questa categoria comprende anche i nuovi tipi di pod automatizzati, navette o veicoli simili. Inoltre, **i regolamenti si applicano anche ai rimorchi che contengono almeno un'unità di controllo elettronico**.

Sicurezza informatica ai sensi della R155



UNECE R 155 definisce i requisiti per la protezione dei veicoli contro gli attacchi informatici. Un punto chiave qui è **l'implementazione di un sistema di gestione della sicurezza informatica (CSMS)** in tutte le aziende che immettono veicoli sul mercato. La cosa entusiasmante è che questo requisito cambia la prospettiva dei produttori. Le loro attività di sviluppo non finiscono più con l'inizio della produzione (SOP). Invece, **c'è un obbligo continuo di controllare i sistemi di sicurezza durante l'intero ciclo di vita di un veicolo, compresi i miglioramenti necessari.**

In questo modo, il legislatore tiene conto della natura altamente dinamica dello sviluppo e della garanzia del software. Inoltre, **il sistema di gestione mira a garantire il rispetto dei requisiti di sicurezza lungo la catena di fornitura. Questo non è un compito facile se si considera che i fornitori rappresentano attualmente oltre il 70% del volume del software**.

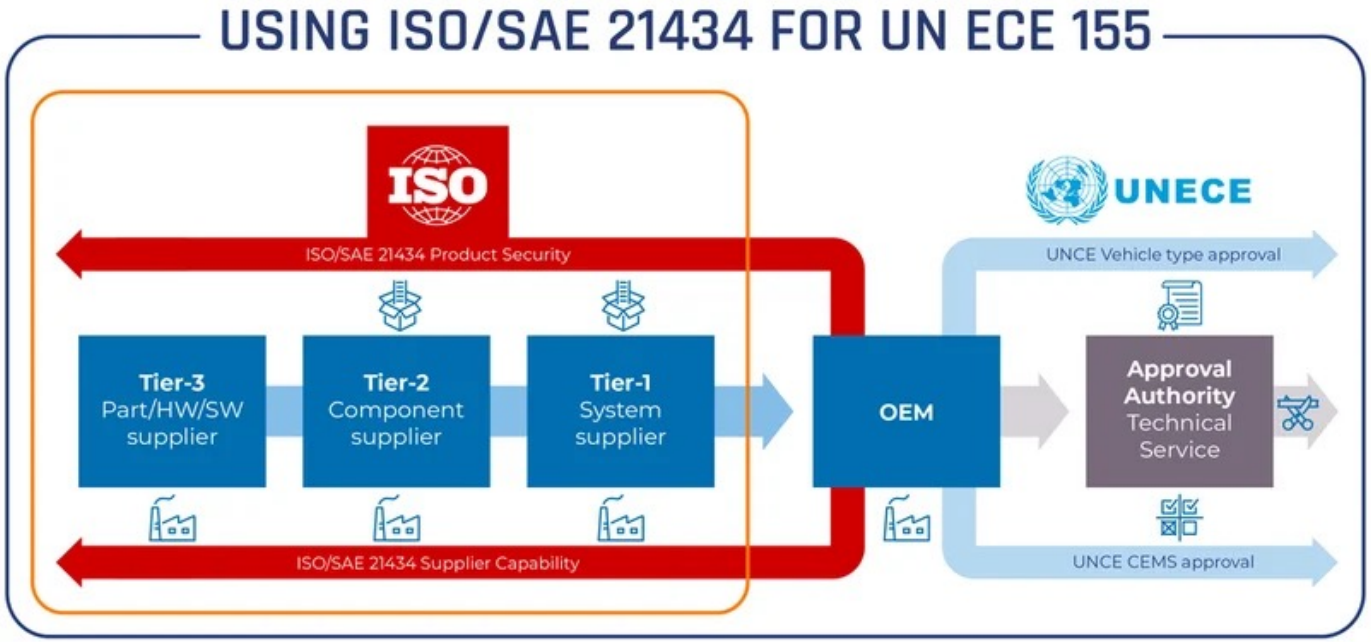
UNECE R 156

Dal momento che i veicoli completamente autonomi parteciperanno anche al traffico nel prossimo futuro, è di fondamentale importanza mantenere il software del veicolo in modo appropriato e mantenerlo costantemente aggiornato, per esempio, attraverso correzioni di bug o aggiornamenti. **La R 156 prescrive quindi l'introduzione e il funzionamento di un sistema di gestione degli aggiornamenti del software (SUMS) conforme alle norme per tutti i veicoli**, che è destinato a fornire una sicurezza permanente per l'intero ciclo di vita di un veicolo.

Sarà necessario installare gli aggiornamenti in modo sicuro e affidabile anche dopo molti anni o decenni. Inoltre, la R 156 pone le basi legali per i cosiddetti aggiornamenti "Over-the-Air" (O.T.A.), che consentono di aggiornare i veicoli con breve preavviso in qualsiasi momento, indipendentemente dalla loro posizione.

ISO/SAE 21434

Secondo i regolamenti UE, i produttori devono garantire la funzionalità dei loro sistemi di gestione in ogni momento e documentare ampiamente lo stato di tutto il loro software.

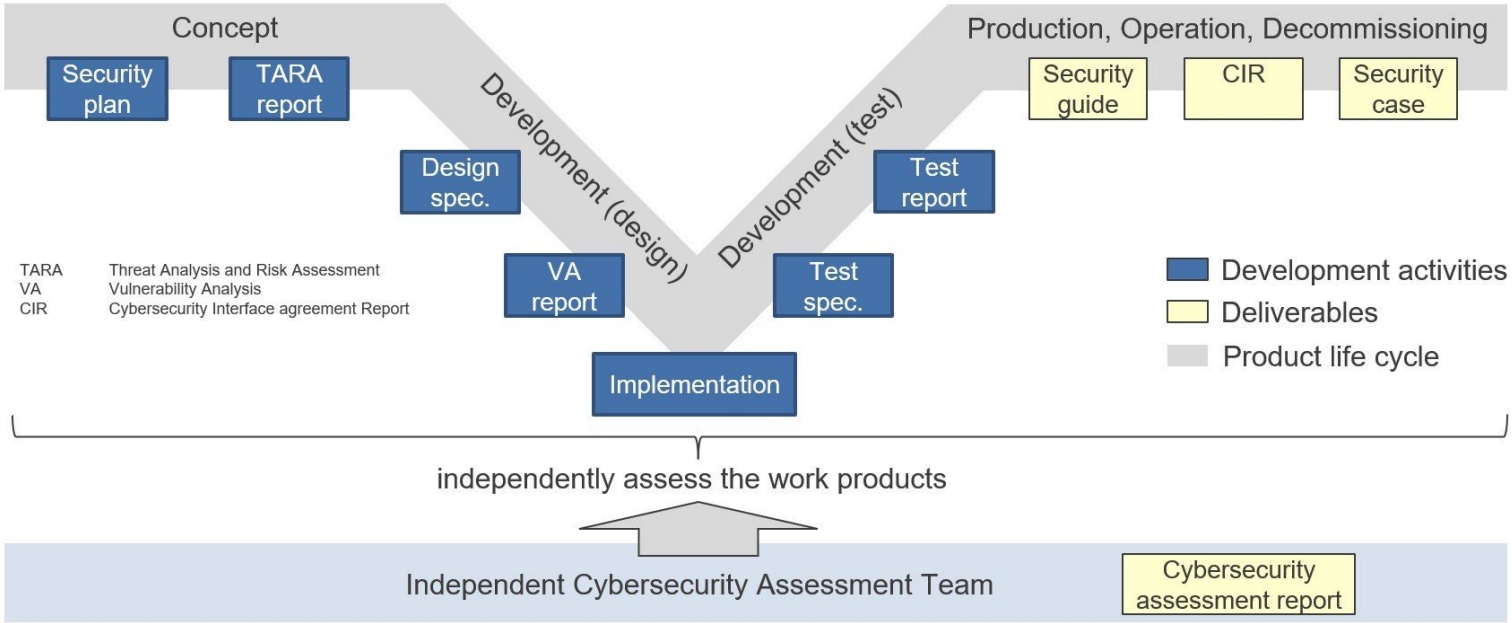


Per fornire uno standard certificabile per la funzionalità di un CSMS, **l'International Organization for Standardization (ISO), insieme alla Society of Automotive Engineers (SAE), ha pubblicato ISO/SAE 21434 nell'agosto 2021**. Negli ambienti professionali, ISO/SAE 21434 dovrebbe fornire una base riconosciuta dalle autorità di approvazione per l'attuazione di un sistema di gestione della sicurezza informatica presso un produttore di veicoli.

ISO/SAE 21434

L'approccio della **ISO 21434**, analogo ai sistemi di gestione comuni come ISO 27001, **richiede l'attuazione di processi e procedure tenendo conto dei rischi identificati**.

L'obiettivo dichiarato della norma è quello di garantire la sicurezza di tutti i sistemi elettrici e, soprattutto, elettronici di elaborazione dati durante l'intero ciclo di vita del prodotto di un veicolo, fino al suo smaltimento.



Conclusioni

- E’ riconosciuto nell'industria che gli attacchi alle automobili stanno aumentando in linea con l'aumento della connettività dei veicoli. **Le aziende automobilistiche e i fornitori di componenti stanno implementando misure di sicurezza avanzate, come l'isolamento dei sistemi critici, l'hardening del software** e l'adozione di standard di sicurezza come l'ISO/SAE 21434.

- E’ chiaro che la sicurezza informatica sta diventando una parte integrante dello sviluppo e della manutenzione dei veicoli moderni, con **industria e ricercatori che lavorano per identificare e mitigare le vulnerabilità in un settore in rapida evoluzione**.

- **E’ fondamentale che centri di competenza come Cyber 4.0 e CIM continuino il loro grande lavoro di supporto alle piccole e medie aziende del settore automotive per metterle in condizione di essere rispondenti alle richieste normative (e soprattutto degli OEM) e di non perdere competitività sul mercato**

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

AUSTRALIA

Sydney NSW | Adelaide SA

EUROPE

Torino ITA | Cuneo ITA | Milano ITA | Genova ITA
Bologna ITA | Roma ITA | Bari ITA | Catania ITA
Sheffield UK | Zurigo CH

USA

New York NY | Cambridge MA

aizoongroup.com
aizoon.com.au
aizoon.us

aizoon@aizoongroup.com

aizoon Technology Consulting
@aizoongroup