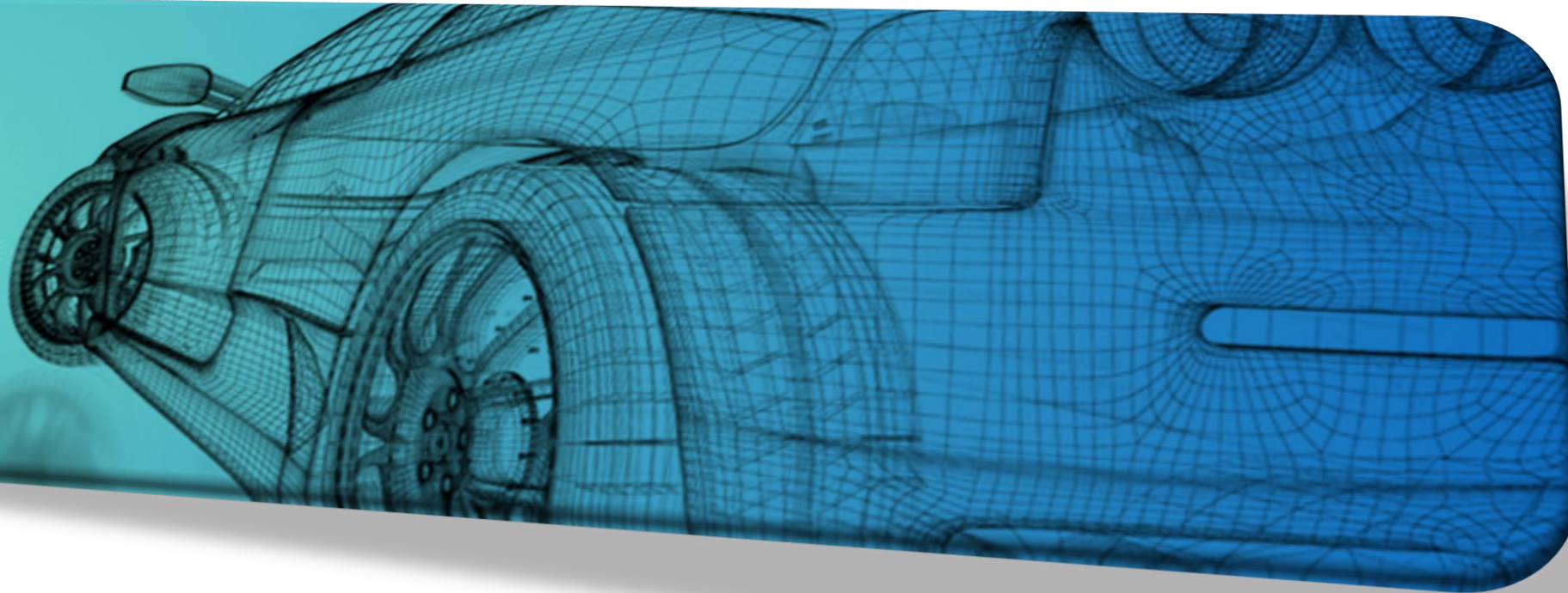


VEHICLE FORENSICS and Infotainment Analysis

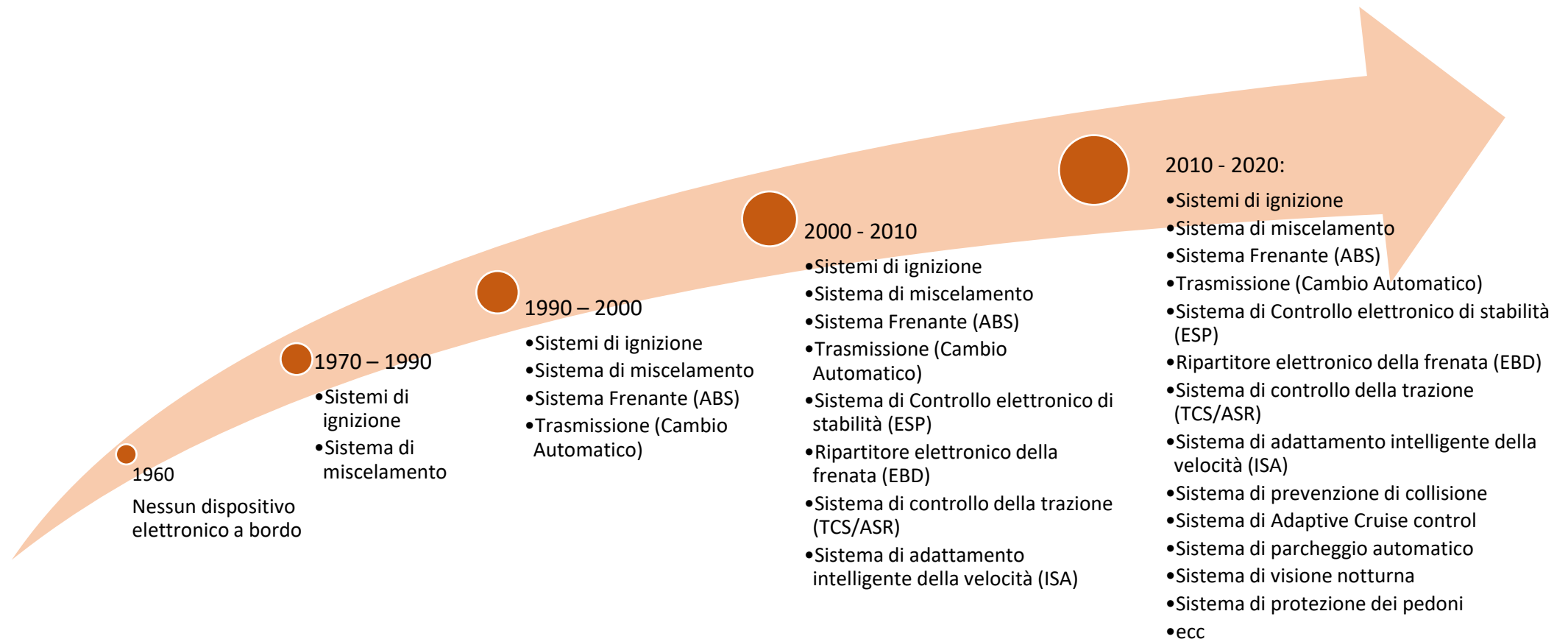


Ing. Claudio Locanto
Forensics Specialist
E-TRACE s.r.l.



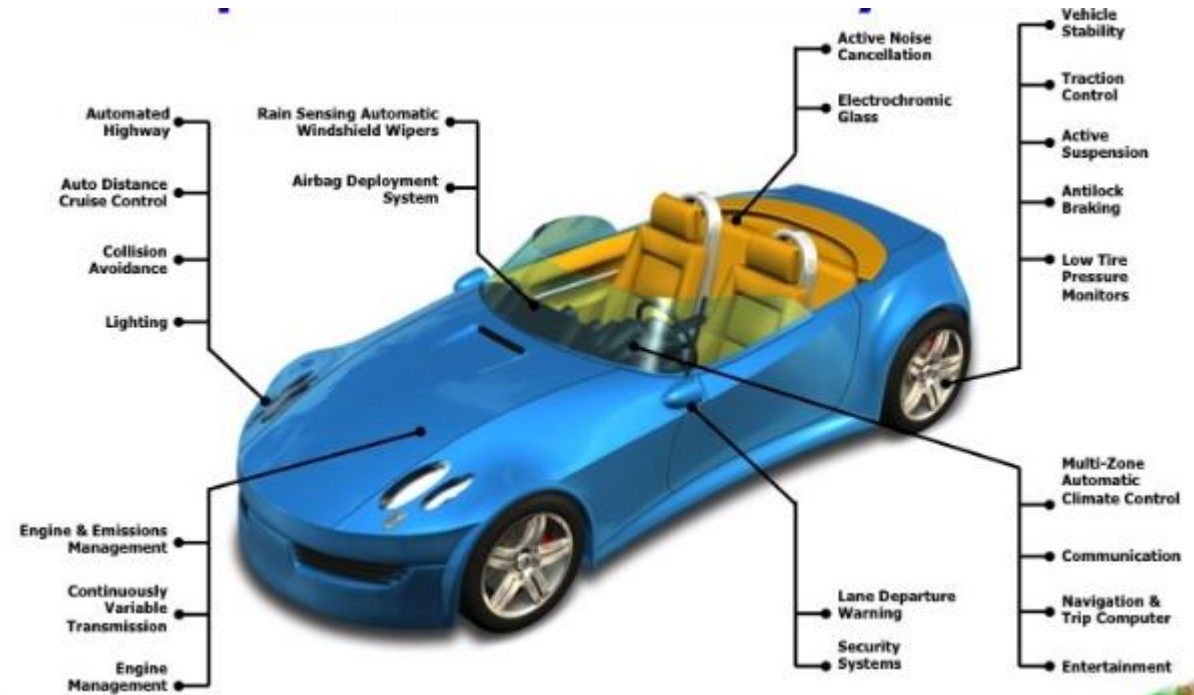
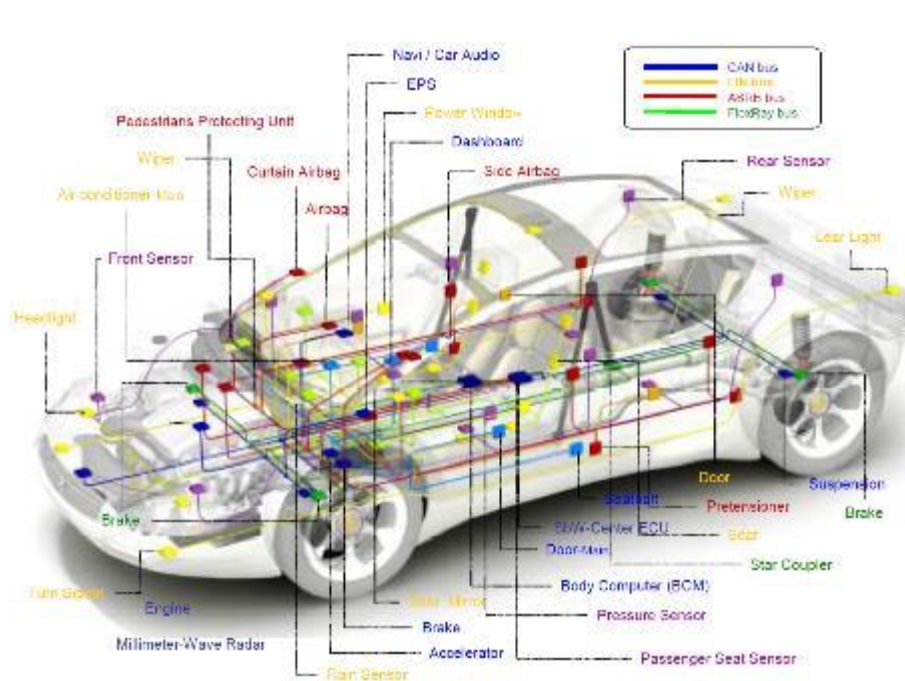
Digital Forensics, Vehicle Forensics

La Vehicle Forensics è la branca delle Scienze Forensi che si occupa della ricerca, acquisizione e analisi della prova informatica relativa a mezzi di trasporto. Negli anni la locuzione Vehicle Forensics è diventata sinonimo dell'attività di analisi atta all'individuazione delle responsabilità in caso di incidente.



ECUs - Electronic Control Unit

In un veicolo moderno possono essere presenti fino a 80 diverse centraline che gestiscono sensori, monitorano e intervengono su diversi processi. Alcune di queste comunicano con altre (V2D), altre con quelle di veicoli vicini (V2V) e registrano diversi tipi di dati

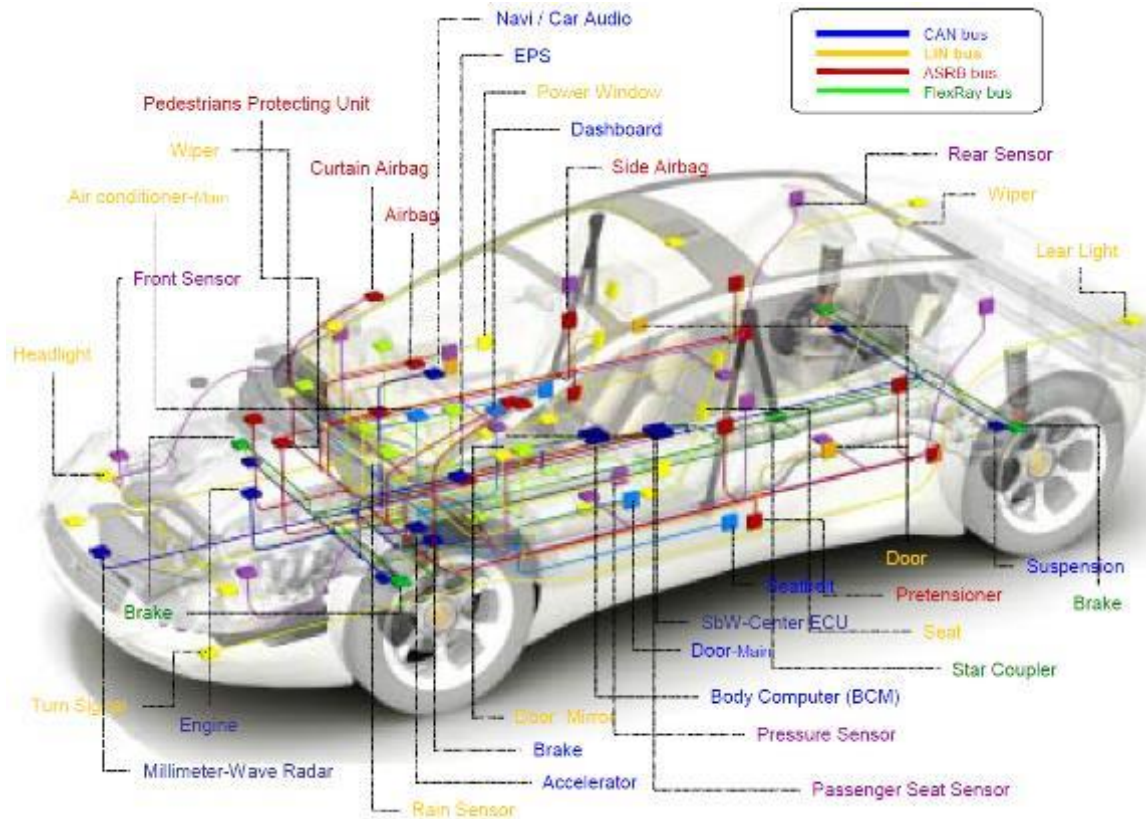


Esempio:

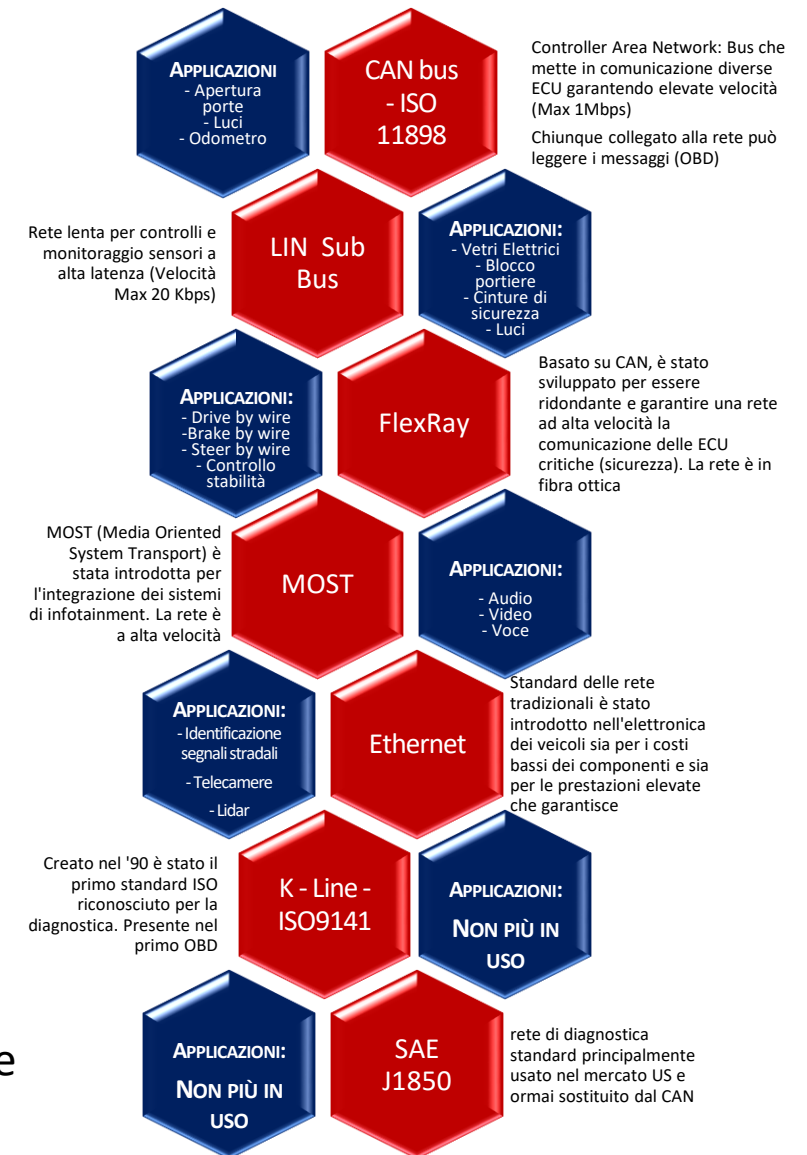
- Centralina AIRBAG (sensore di accelerazione) comunica con pretensionatore cinture. In caso di brusche frenate alcune centraline salvano alcuni parametri su memorie NAND
- Centralina ABS (sensore di velocità delle ruote) comunica con il sistema frenante.
- Centralina ECU/ECM (Engine Control Unit/Module) riceve dati dal CAN Bus elaborando i dati per ottimizzare le performance del motore e registrare eventuali malfunzionamenti.

Network and Protocols

Le ECUs possono essere connesse a diverse reti presenti all'interno dei veicoli:



Per aumentare la sicurezza sono stati introdotti dei dispositivi Gateway che permettono la connessione di diversi dispositivi a più reti



Sistemi Informativi

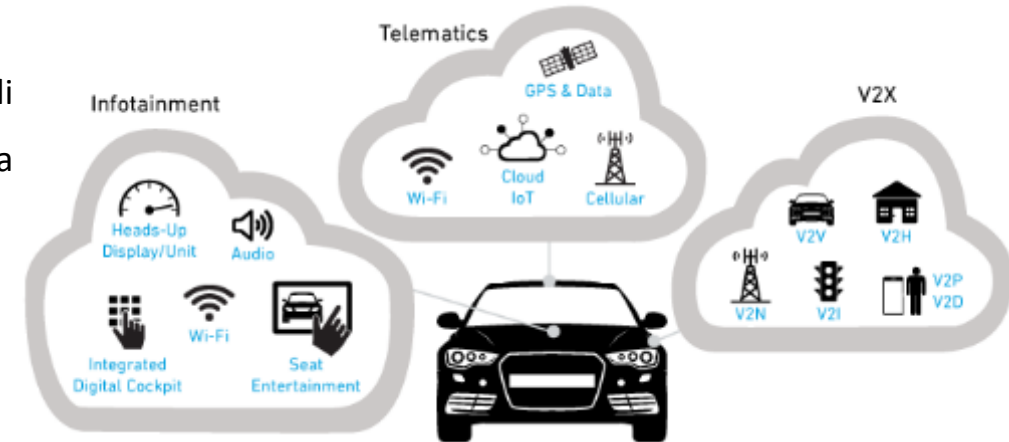
Le diverse centraline elettroniche (ECU) a bordo delle autovetture possono lavorare su dati in streaming provenienti dalle varie reti ma possono anche salvare dati che possono essere interessanti ai fini probatori anche in casi non strettamente legati agli incidenti stradali

INFOTAINMENT:

- Sistema che permette agli utenti di interagire direttamente con il veicolo e che fornisce agli stessi informazioni in tempo reale sulle performance, sulla manutenzione da effettuare ma più in generale **essendo connesso a internet** al proprio mondo digitale

TELEMATICS:

- Integrazione tra i sistemi di telecomunicazione e informativi in base alle scelte del produttore ma che sostanzialmente forniscono servizi di Vehicle-to-Infrastructure (V4I) o di Vehicle-to-Vehicle (V2V); ne sono un esempio le blackbox installate dalle compagnie assicurative o da produttori per integrare i servizi di assistenza SOS



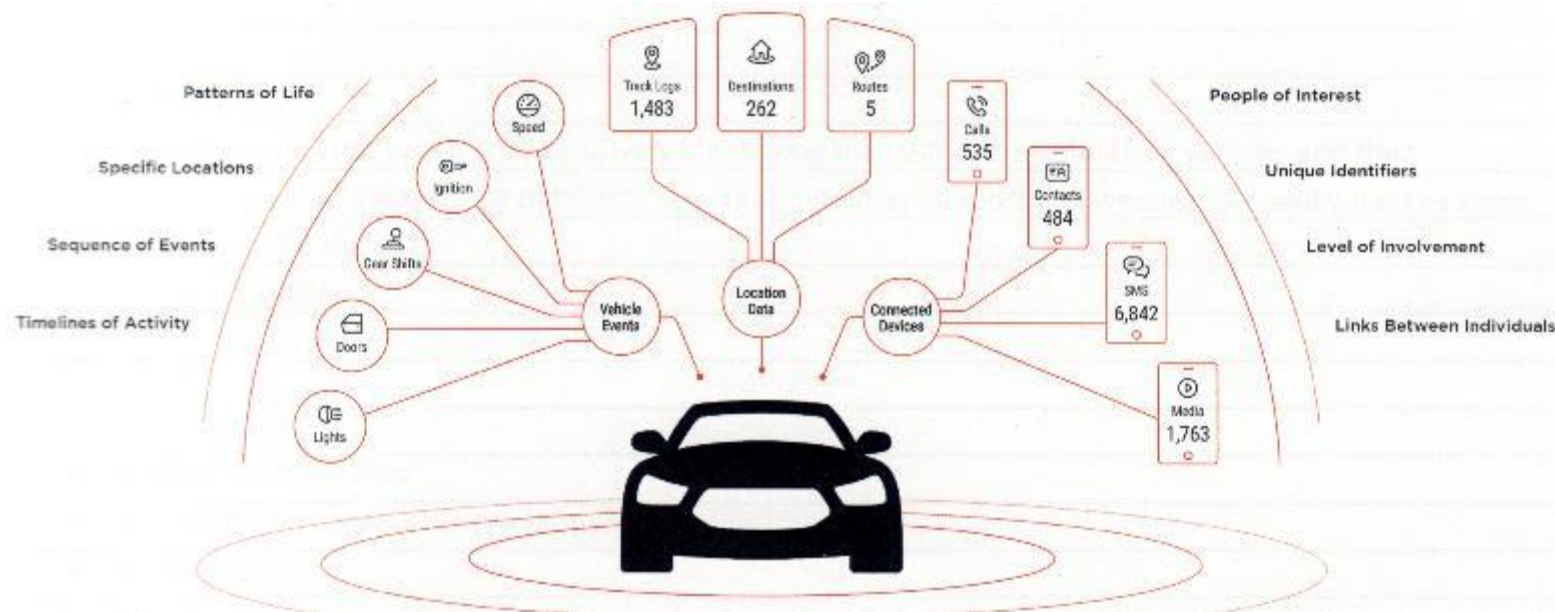
I dati provenienti dai sistemi di Infotainment presenti su quasi tutti gli autoveicoli sono diventati dei collettori di informazioni provenienti da diversi sistemi e dispositivi.

Infotainment, Telematics e Telemetria

Il sistema di Infotainment permette all'utente da un lato di interagire con il proprio spazio digitale e dall'altro di interagire con il sistema di telemetria del veicolo e quello telematico e in futuro a quello V2X.

Su alcuni veicoli, è presente già da tempo uno slot per SIM per la connessione alla rete LTE che viene direttamente gestita dai dispositivi di Infotainment (AP Wifi)

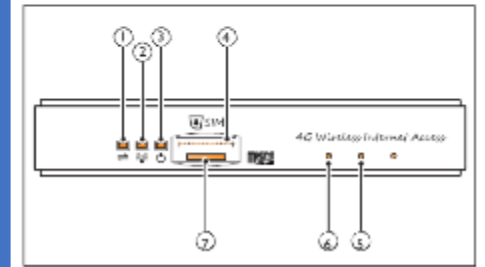
Il sistemi di diagnostica del veicolo (ospitati originariamente in rete air-gapped) viene connesso direttamente o indirettamente al sistema di infotainment



Wi-Fi router front panel

4G router

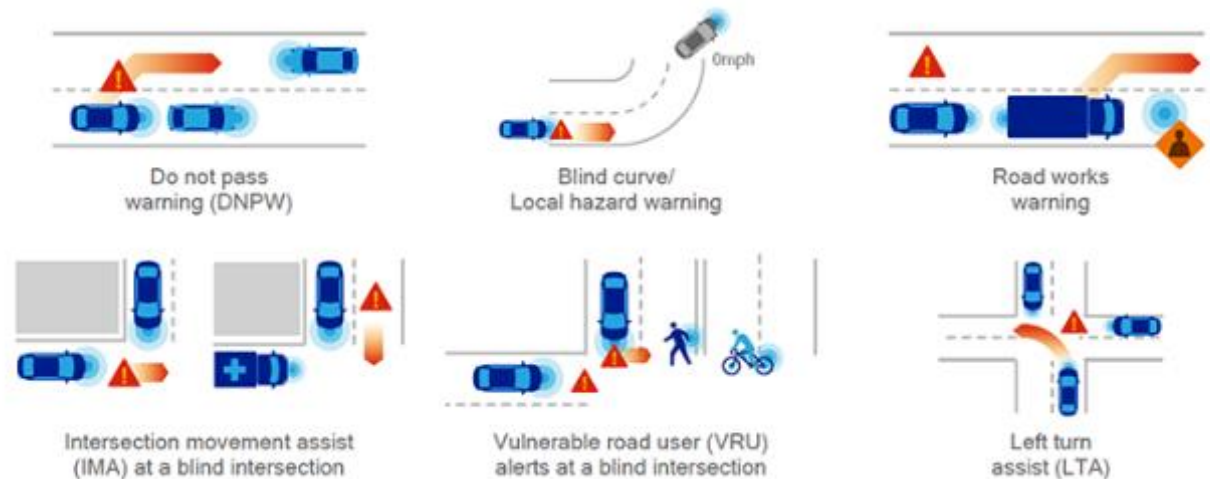
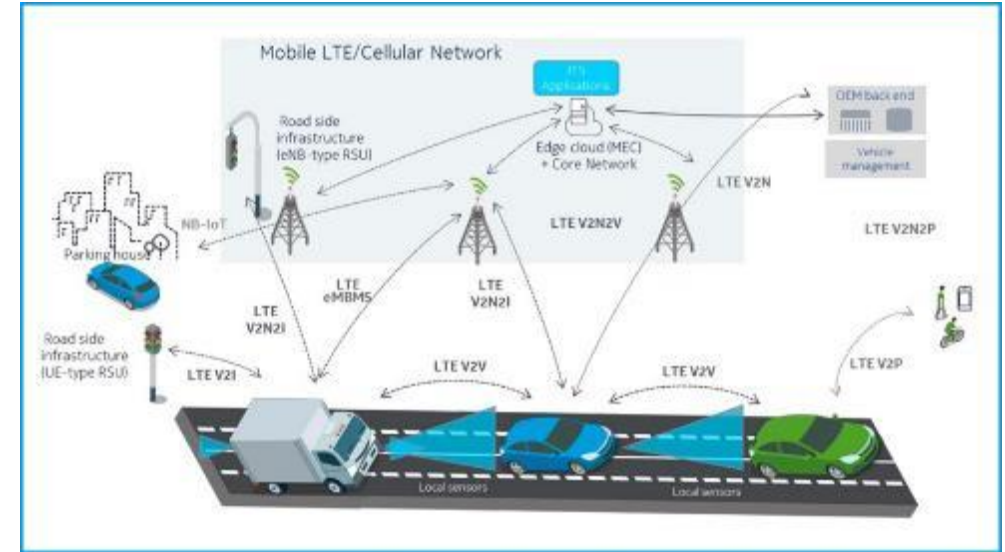
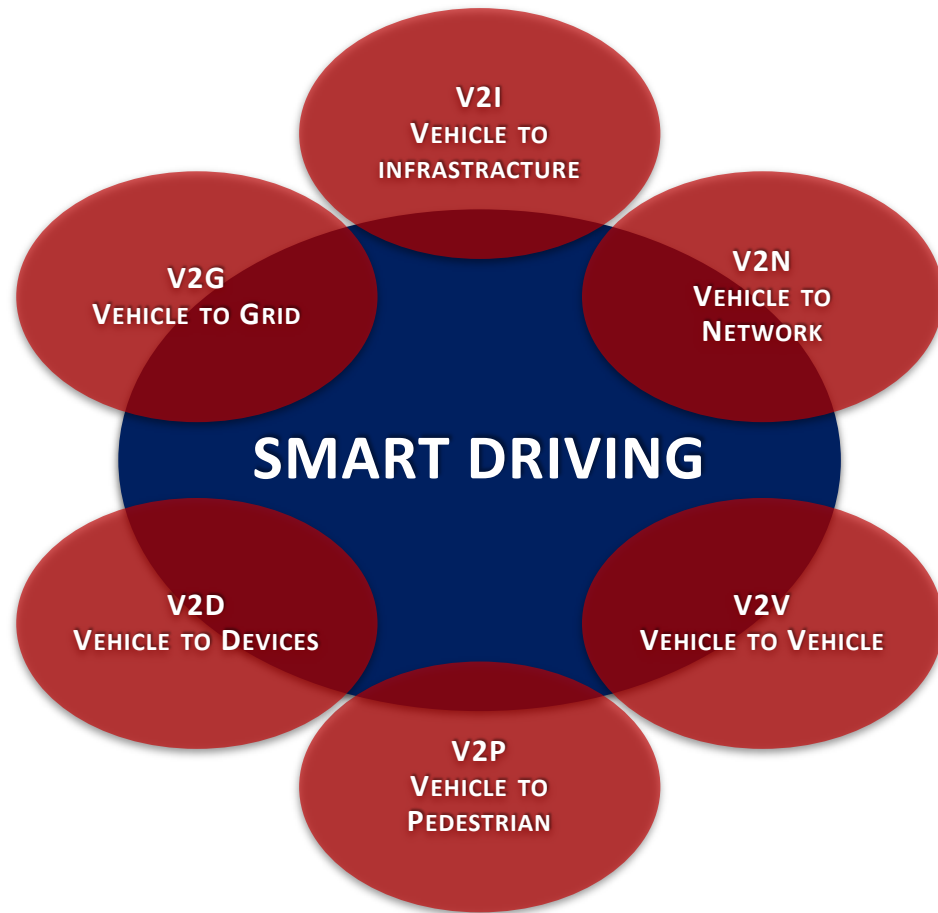
- 1 Internet/4G LED
- 2 WLAN LED
- 3 Power LED
- 4 SIM card slot
- 5 Firmware reset button
- 6 Reset button (restart)
- 7 Micro SD card slot



Sul sistema di infotainment confluiscono numerosi dati provenienti dai diversi sistemi, in real time e a seconda del tipo di veicolo, possono essere salvati all'interno della memoria interna/esterna che in alcuni casi (Mercedes, BMW) è sotto forma di hard disk magnetico

SMART Driving

Un notevole impulso all'elettronica onboard è dato dai sistemi a guida autonoma che richiedono per il loro funzionamento dati in realtime raggruppati nei seguenti sistemi:



Uber Eats self-driving accident

Domenica 18 marzo 2018 in serata intorno alle 22.m., a Tempe, in Arizona, un'auto a guida autonoma Uber Volvo, contenente un operatore di riserva umano al volante, si è imbattuta e ha ucciso una pedone, la 49enne Elaine Herzberg, che era entrata in strada fuori da un passaggio pedonale e nella parte anteriore dell'auto a guida autonoma in arrivo



✓ FORENSIC ANALYSIS OF UBER Self Driving Car



FCA richiama 1,4 milioni di vetture negli Usa per paura di un attacco hacker

In calo il titolo a Piazza Affari

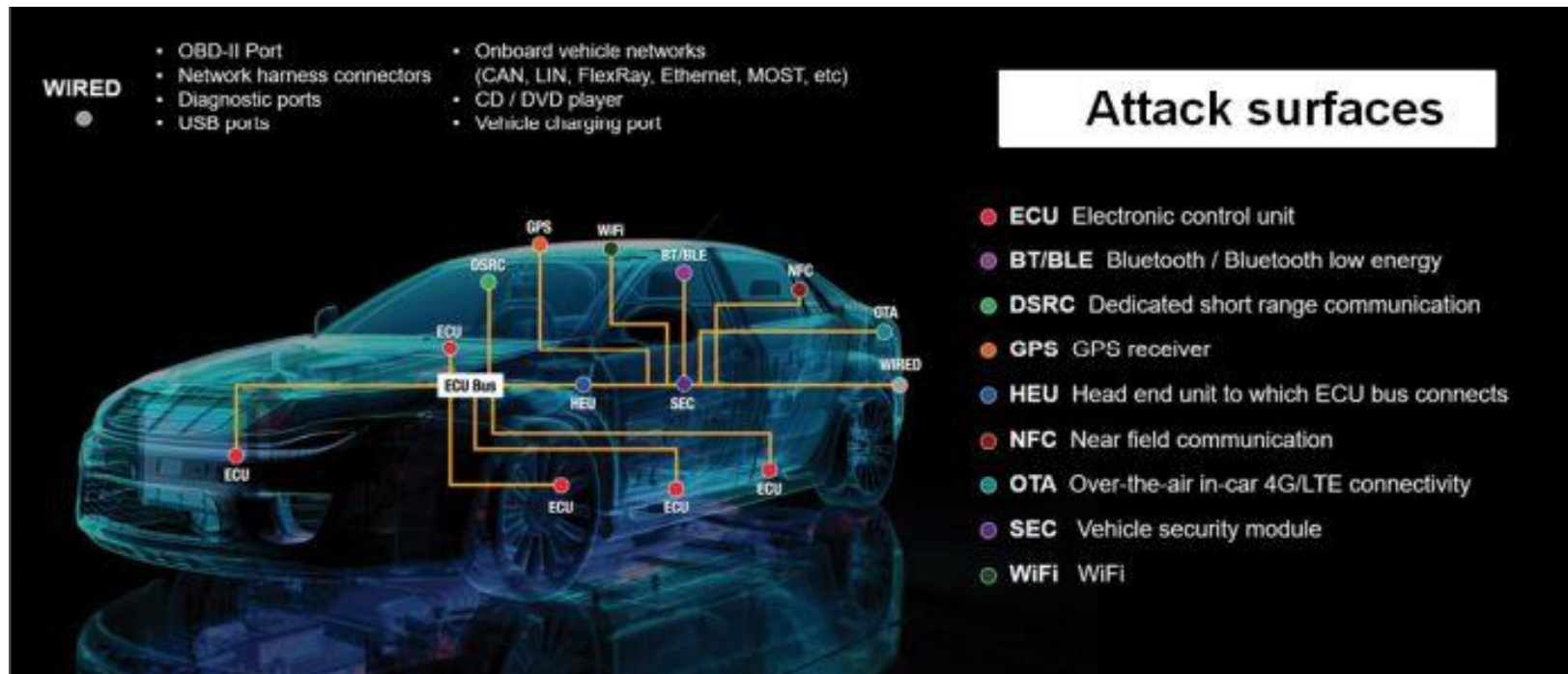
MOBILITÀ



FCA richiama altre 7.810 Jeep vulnerabili ad attacchi informatici



Superfici di Attacco



Reti basate su protocolli non sicuri + Ampie superfici di attacco
=
Rischio elevato su tutti i veicoli attualmente circolanti

Non solo FCA



Servizi acquistati



Apple CarPlay

Acquistato fino al: 09/12/2021

[> Dettagli](#)



Remote Services

Acquistato

[> Dettagli](#)



Real Time Traffic Information

Acquistato fino al: 09/12/2021

[> Dettagli](#)



Chiamata d'emergenza intelligente

Acquistato

[> Dettagli](#)



BMW Online

Acquistato fino al: 09/12/2021

[> Dettagli](#)



TeleServices

Acquistato

[> Dettagli](#)



Concierge Services

Acquistato fino al: 09/12/2021

[> Dettagli](#)

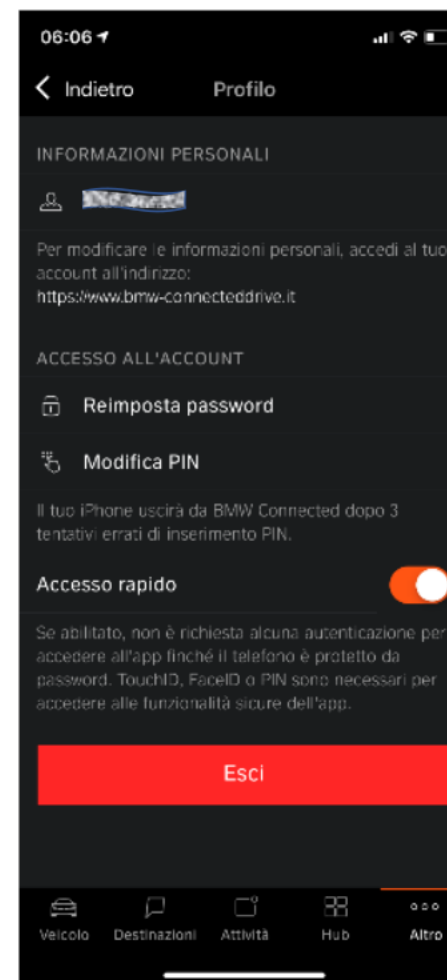
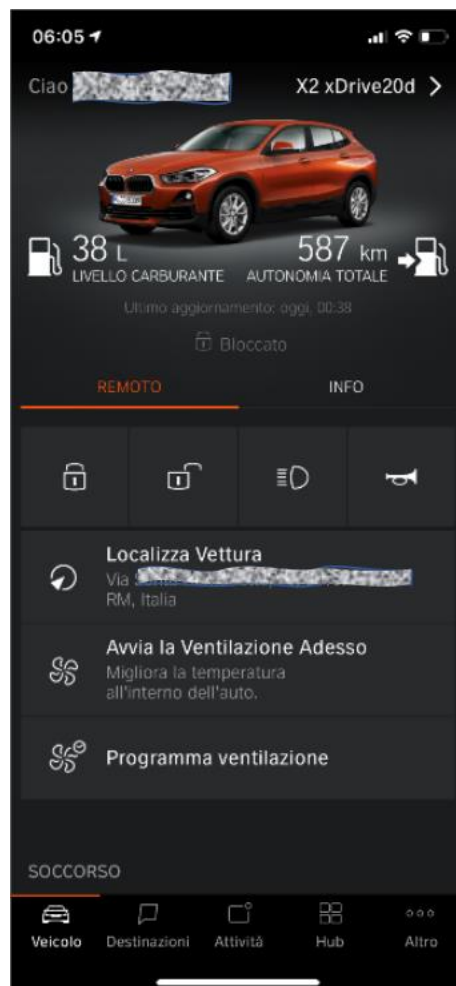


ConnectedDrive Services

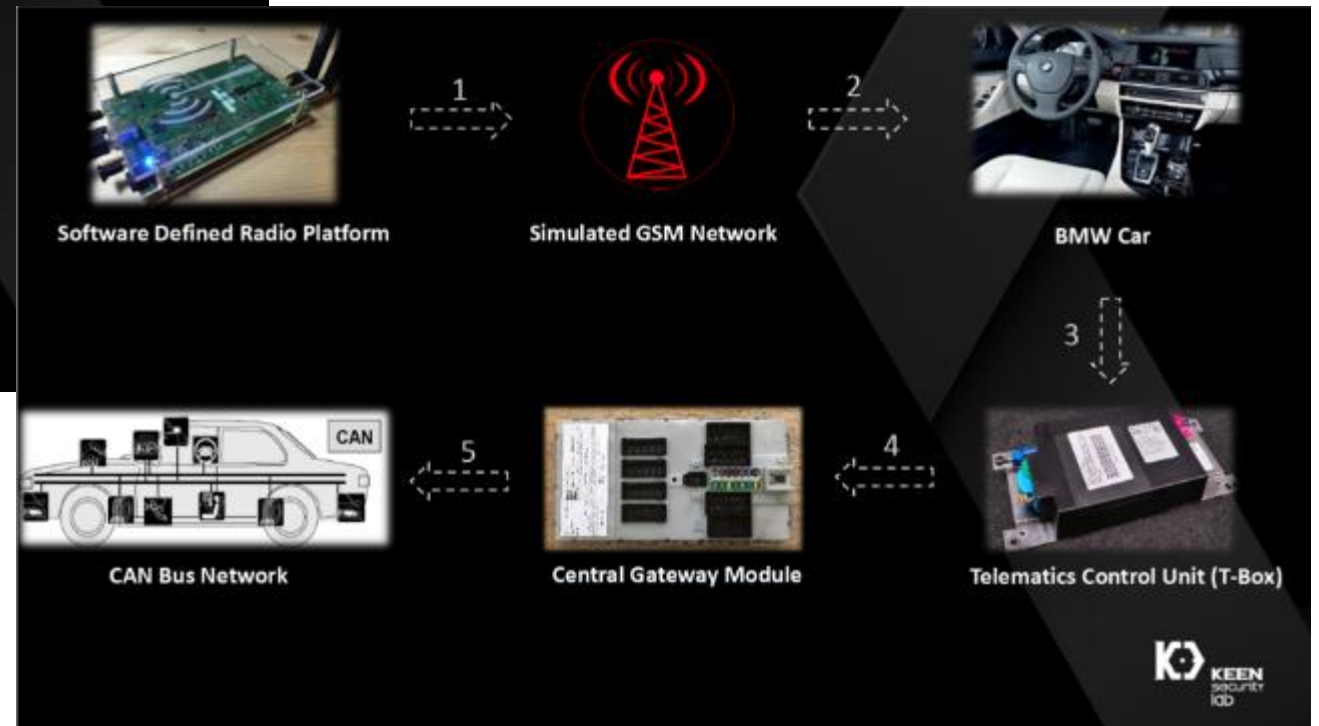
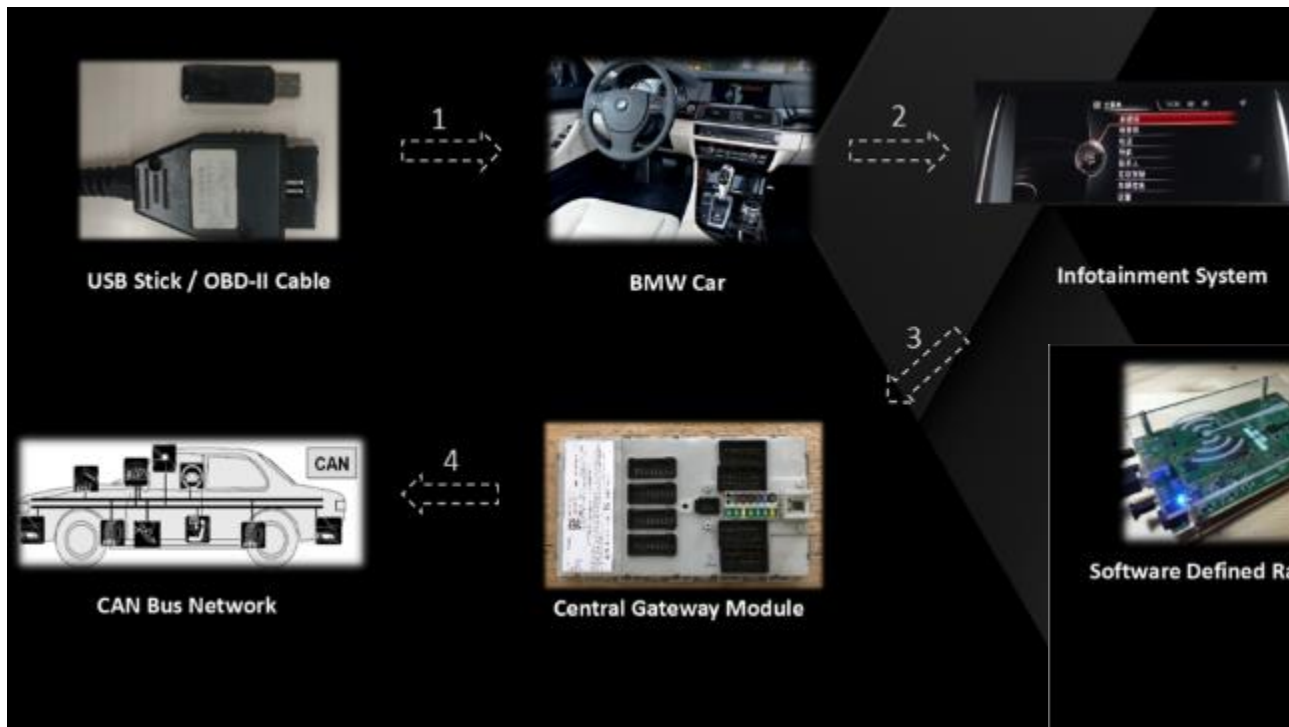
Acquistato

[> Dettagli](#)

✓ BMW CONNECTED



✓ BMW CONNECTED



<https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/>

✓ BMW CONNECTED

No.	Vulnerability Description	Access	Affected Components	Reference
1	All the detail information has been reserved due to security concerns.	Local (USB)	HU_NBT	CVE-2018-9322
2		Local (USB/OBD)	HU_NBT	
3		Remote	HU_NBT	Logic Issue
4		Remote	HU_NBT	Reserved
5		Local (USB)	HU_NBT	CVE-2018-9320
6		Local (USB)	HU_NBT	CVE-2018-9312
7		Remote (Bluetooth)	HU_NBT	CVE-2018-9313
8		Physical	HU_NBT	CVE-2018-9314
9		Physical	TCB	Reserved
10		Remote	TCB	Logic Issue
11		Remote	TCB	CVE-2018-9311
12		Remote	TCB	CVE-2018-9318
13		Indirect Physical	BDC/ZGW	Logic Issue
14		Indirect Physical	BDC/ZGW	Logic Issue



<https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/>

✓ BMW CONNECTED

Autobombe a controllo remoto



Inside IS Weapons Lab



<https://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883>

Frammentazione dei sistemi

- La società decide che tipo di sistema deve essere presente su diversi modelli
- Modelli e marchi molto diversi in termini di costo e prestigio possono condividere lo stesso sistema di Infotainment (Es. Gruppo FCA monta sistemi simili su Fiat 500x e JEEP Grand Cherokee)
- Alcune Aziende possono consorziarsi per condividere tecnologie e pertanto lo stesso sistema può essere montato su marchi non facenti parte dello stesso gruppo

Esempio Alleanza Renault-Nissan-Daimler

- GM condivide la tecnologia con Nissan
- Nissan monta un sistema su alcuni suoi modelli e condivide la propria tecnologia con Renault
- Renault la monta su alcuni suoi modelli e la condivide col gruppo Daimler che la monta sulla serie GLA
- Dacia del Gruppo Renault invece monta un sistema custom basato sul LG (Opensource)



Gestione UPDATE dei sistemi connessi quasi nulla

Approccio *Vendi e Dimentica*. La gran parte dei veicoli riceve aggiornamenti solo al momento dei Tagliandi (annuali)

Qualche buona notizia... le ISO

ISO/SAE 21434, Road vehicles – Cybersecurity engineering: fornisce uno standard sulla sicurezza informatica nell'ingegneria dei sistemi elettrici ed elettronici (E/E) all'interno dei veicoli stradali. Aiuterà i produttori a stare al passo con le mutevoli tecnologie e i metodi di attacco cibernetico, e definisce il vocabolario, gli obiettivi, i requisiti e le linee guida relativi all'ingegneria della cybersecurity per una comprensione comune in tutta la catena di fornitura

ENISA good practices for security of Smart Cars: definisce le best practices per la sicurezza delle auto intelligenti, vale a dire i veicoli connessi e (semi)autonomi, fornendo caratteristiche a valore aggiunto al fine di migliorare l'esperienza degli utenti di auto e migliorare la sicurezza dell'auto. Fa il punto su tutte le iniziative di standardizzazione, legislative e politiche esistenti, mirando a essere un punto di riferimento per promuovere la cybersecurity per le auto intelligenti (auto connesse e automatizzate) in tutta Europa e aumentare la consapevolezza sulle minacce e sui rischi rilevanti con un focus sulla "cybersecurity per la sicurezza".

Introducono tra gli altri i concetti di

- ✓ Progettazione dei nuovi sistemi mediante il paradigma Security by-Design
- ✓ Obbligo per i produttori di fornire aggiornamenti continui (OTA)



Acquisizione Forense ECU

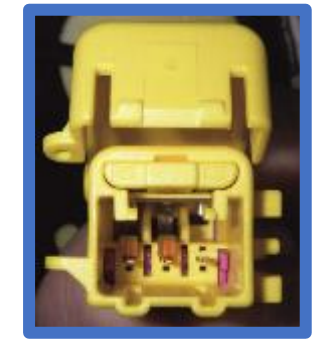
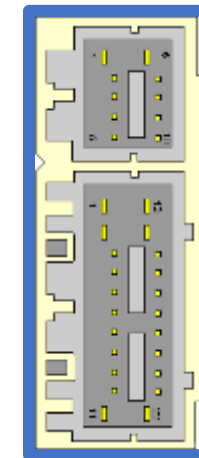
In mancanza di uniformità nella Legislazione internazionale che vincoli le case automobilistiche a standardizzare i dispositivi montati sulle vetture l'acquisizione e l'analisi delle ECU presenta diverse difficoltà:

- ECUs altamente specializzate per ogni funzione/sensore
- Eccetto OBDII, mancanza di connettori standard.
- Elevato numero di Network
- Elevato numero di Bus e protocolli di rete



Per la ricostruzione degli incidenti vengono acquisiti i dati che vengono salvati sulle ECU ABS o Airbag

Il sistema di Infotainment, a secondo dei modelli è quello che riesce a interfacciarsi con il maggior numero di sistemi onboard è spesso è dotato di uno spazio di storage molto elevato



Acquisizione dati EDR (ricostruzione incidenti)

CRASH DATA (Event Data Records):

- PRE-CRASH
- DEPLOYABLE EVENTS
- NON DEPLOYABLE EVENTS
- POST- CRASH



Vehicle Forensics – Acquisizione Infotainment

L'acquisizione di un sistema di infotainment permette di accedere a una serie di dati non solo telemetrici e legati al veicolo ma anche legati ai dispositivi connessi (smartphone dei passeggeri). Viene effettuata attraverso soluzioni HW/SW commerciali come IVE BERLA



1. IDENTIFICATION
2. ACQUISITION
3. ANALYSIS

La soluzione include :



L'esportazione può essere importata all'interno di programmi di analisi forense di dispositivi **mobile** come MSAB XRY per incrociare i dati

MSAB

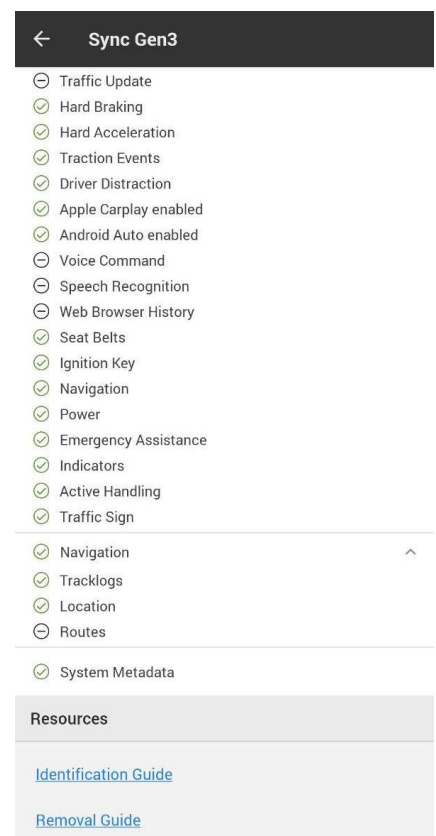
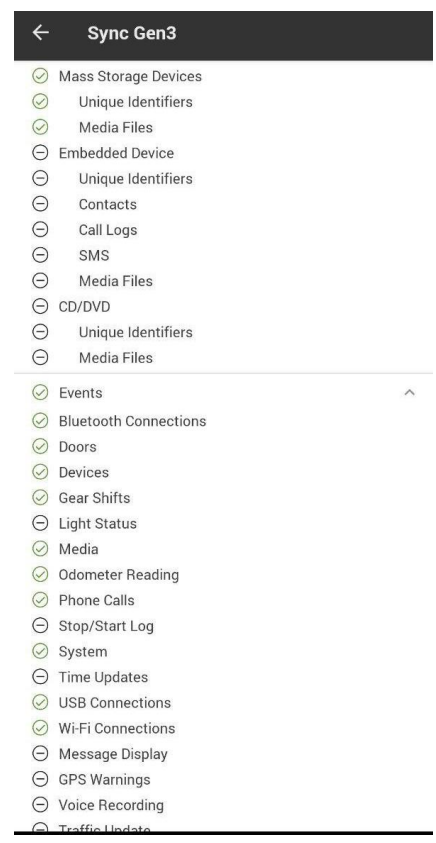
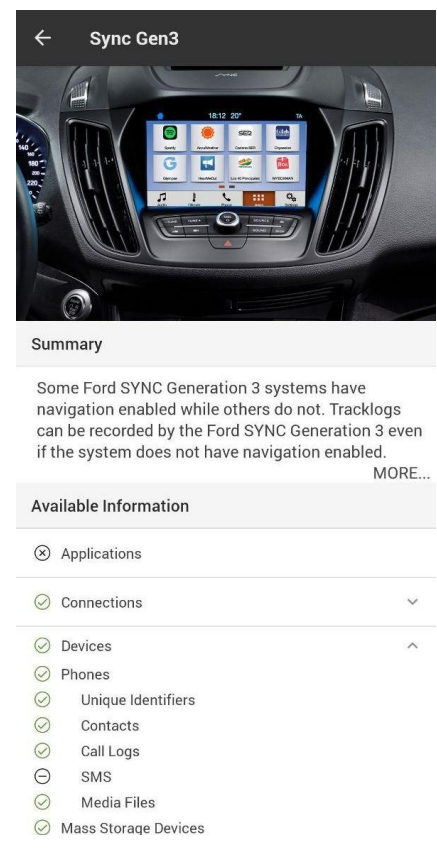


A Proposito di Berla, Ford e sicurezza dei dati Utente



Ford Motor Company uses its infotainment system to secretly download and store drivers' private text conversations, and then turns them over to law enforcement and the private company Berla, a new class action lawsuit alleges.

<https://topclassactions.com/lawsuit-settlements/consumer-products/auto-news/1032062-ford-motor-co-accused-of-violating-privacy-law-by-storing-drivers-private-conversations-and-releasing-them-to-cops-and-a-private-company-a-new-class-action-lawsuit-alleges/>



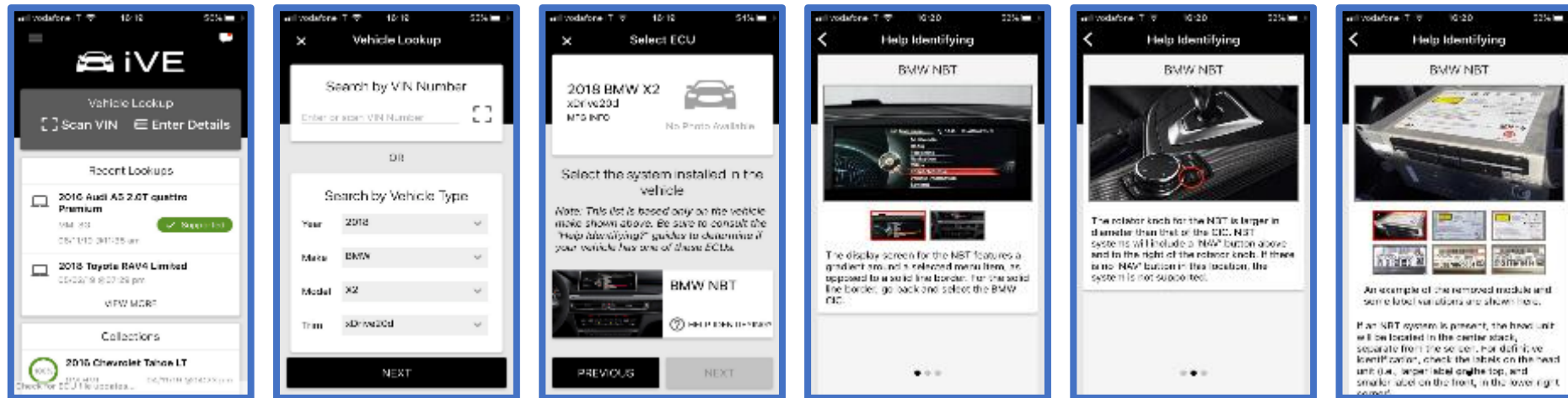
Step 1: Identification

Attraverso il processo di identificazione è possibile riconoscere il sistema in questione senza doverlo smontare fisicamente dal veicolo.

L'identificazione avviene a partire dal codice internazionale del telaio (VIN) o dai dati di immatricolazione del veicolo con diversi strumenti messi a disposizione da BERLA:

- IVE Berla PC software
- Mobile App (in iOS and Android marketplaces)
- Sul sito <https://berla.co/vehicle-lookup>

Screenshot dell'app iOS

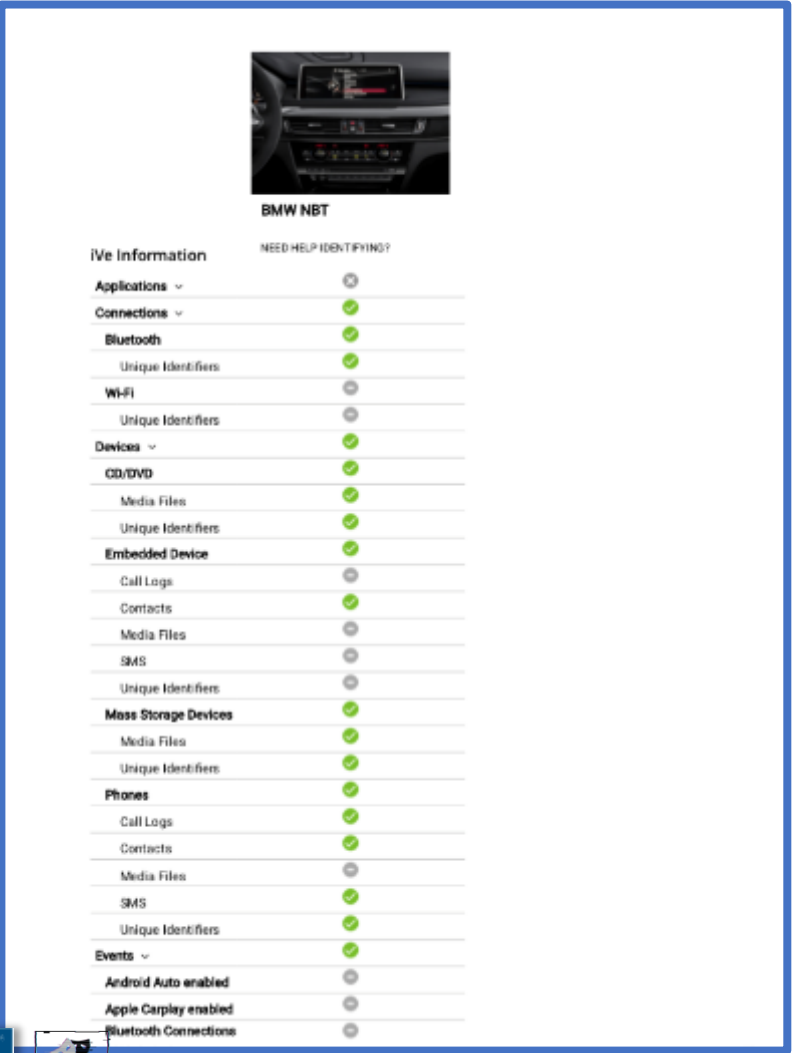


Al termine del processo viene fornito



Step 1: Identification

Through the Vehicle Lookup function it is possible to identify which data is available for this vehicle



Screenshot della funzione di Vehicle
lookup sul sito ufficiale

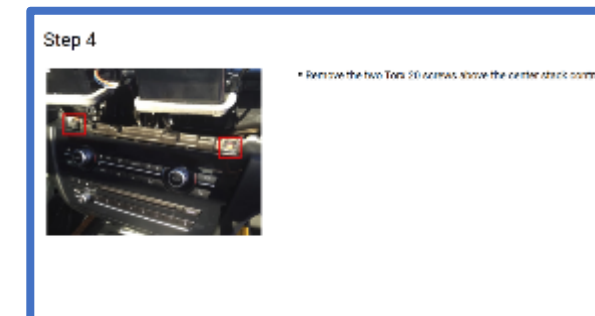
Step 2: Acquisition – 1/3

Ogni dispositivo supportato deve essere acquisito
con il proprio hardware dedicato, fornito da Berla:

- | | |
|-------------------------------------|--|
| • Device Interfaces Boards (DIB) | Dispositivi Specifici: |
| • Cavi Specifici (Eth0-USB adapter) | |
| • Cavi Generici OBDII | |
| | <ul style="list-style-type: none">• TCT• BDM• Cavo USB• Single Board Computer (SBC) |

Alcuni dispositivi possono essere acquisiti senza smontare il dispositivo stesso dalla dashboard.

IVE offre istruzioni dettagliate su come smontare le apparecchiature con testo e immagini



Step 2: Acquisition – 2/3



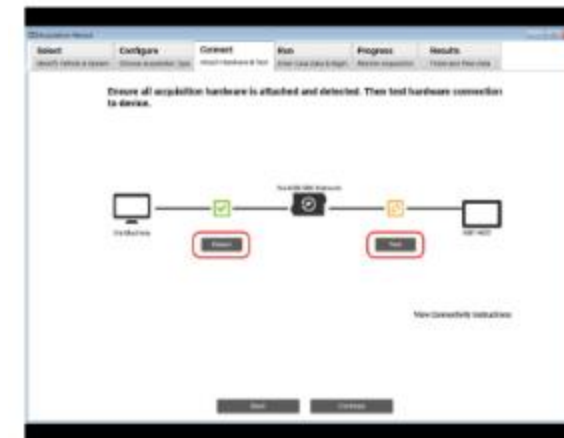
- Within the iVe software, start a new collection and enter the vehicle information.
- The NBT ECU option is available when selecting BMW, MINI, or Rolls-Royce for the make.
- Select 'Continue.'



- Select 'Logical' for the acquisition type on the 'Configure' screen.

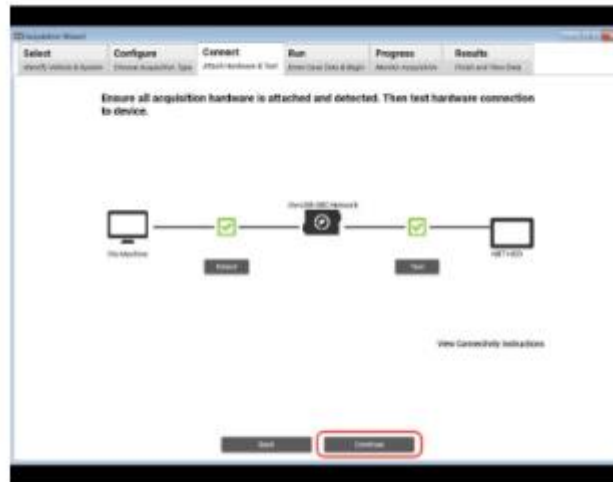


- In the empty 'Acquisition Options' text boxes on the 'Configure' screen, enter the following information for the NBT hard drive: MAC address, Bluetooth MAC address, serial number, and SNR.
- Some or all of the numbers might be found on the NBT module's label, though label formats can vary.
- Note: As seen in the second photo, the serial number may be printed both under the bar code and also above and below the QR code (broken into two segments).
- If two different MAC address are NOT listed, see the troubleshooting section of the iVe user guide for instructions on obtaining the MAC addresses through alternative means.
- For iVe software versions older than 2.1.1, the MAC address retrieval instructions are not included in the user guide. In such cases contact Berla support for instructions on getting the MAC addresses from the unit.
- Once all the numbers have been entered, select 'Continue.'



- Confirm successful hardware connectivity by clicking the 'Detect' button, and after it passes, clicking the 'Test' button.
- When the 'Test' button is clicked, iVe attempts to unlock the drive for performing the acquisition.

Step 2: Acquisition – 3/3



- Once both tests have passed successfully, click 'Continue.'



- Enter case info on the 'Run' screen (optional).
- Select 'Continue' to start the acquisition.



- While the acquisition is in progress, the status may be monitored on the 'Progress' screen.



- Once the acquisition has completed, the 'Results' screen appears.
- Select the 'Go to Workspace' button to begin viewing the acquired data.

Grazie per l'attenzione

