13W-AutoSPIN

Automotive Cybersecurity

Challenges and opportunities

Alessandro Farsaci (CNH industrial)
Cosimo Senni (Magneti Marelli)

Milan, Italy

November 12th, 2015

Agenda

Automotive Cybersecurity

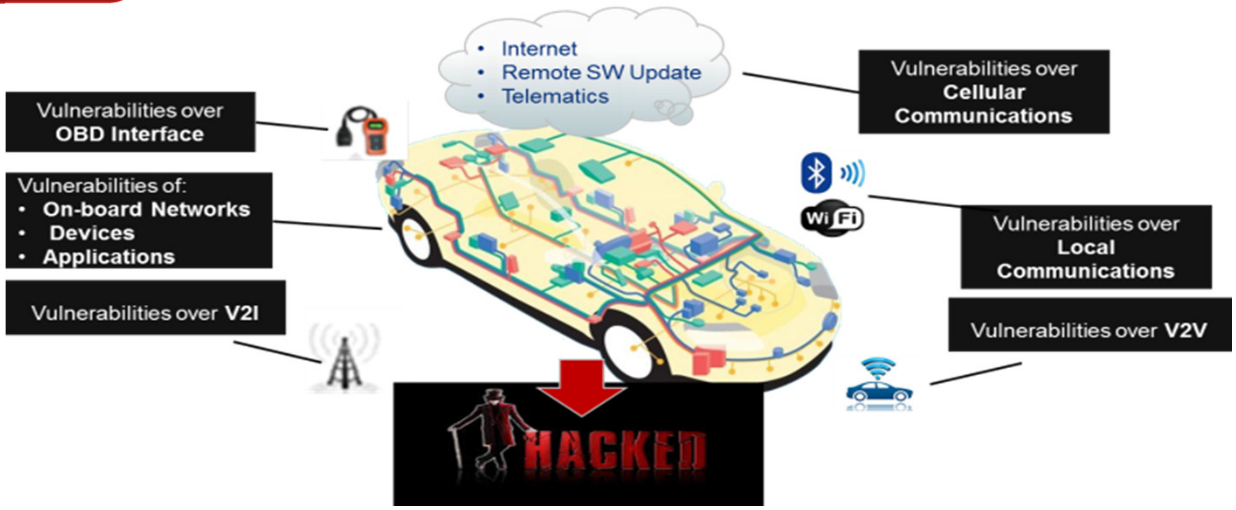
- Overview
- Recent issues
- Possible impacts
- OEM point of view
- Tier1 point of view
- Conclusion

Automotive Cybersecurity

Overview – Cybersecurity Use cases

Interaction of internet world with the in-vehicle network

Security risks including Cyber attacks targeting vehicle functionality and maneuverability



- Internet
- Remote SW Update
- Telematics

Vulnerabilities over **OBD Interface**

Vulnerabilities of:
- **On-board Networks**
- **Devices**
- **Applications**

Vulnerabilities over **V2I**

Vulnerabilities over **Cellular Communications**

Vulnerabilities over **Local Communications**

Vulnerabilities over **V2V**

(GSMa) - Forecast is to have all cars connected to the Internet by 2025

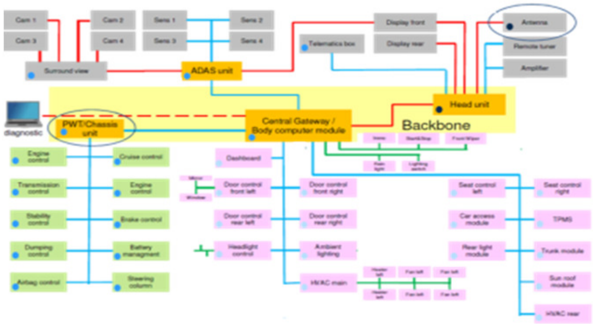
Similar scenario to what happened in PC world in the nineties

Automotive Cybersecurity

Overview – Attacks and attackers

New **attacks not requiring specific automotive expertise**

- **Attacks impacting main vehicle functionality**
  - **Safety attack – cause an *issue* to someone or to the society**
  - **Privacy attack – steal personal information and make business on that**
  - **Image attack – cause faults in the vehicle of a selected OEM to cause an expensive recall**



Standard **attacks requiring automotive experience**

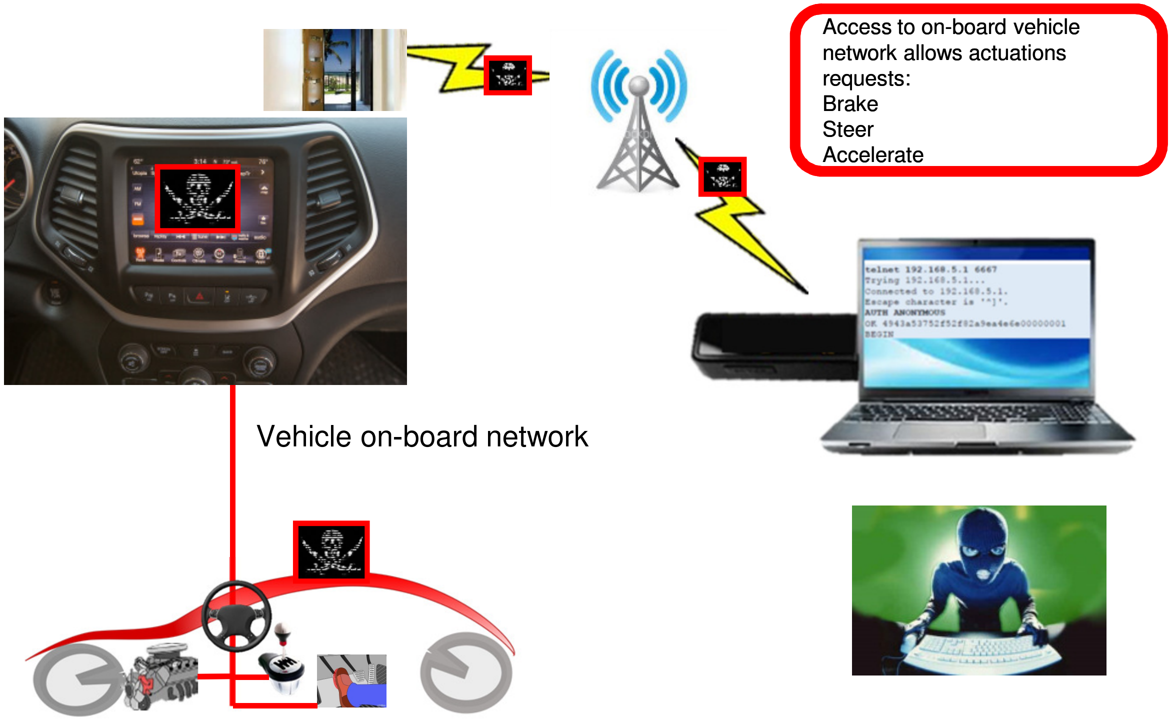
- **Chip tuning and unauthorized ECU replacement:**
  - **Replace an ECU with an unauthorized ECU(Business Abuse)**
  - **Tune an existing ECU with illegal parameters or replace its firmware**
- **Vehicle theft**
  - **Use of counterfeit/stolen parts**
  - **Connect to the OBD port in order to disable anti-theft measures.**
  - **Cracking of vehicle immobilizer**

Automotive Cybersecurity

Overview – Typical attacks

Gain access to vehicle internal network

Inject *regular* commands with malicious purposes



Access to on-board vehicle network allows actuations requests:
Brake
Steer
Accelerate

```
telnet 192.168.5.1 6667
Trying 192.168.5.1...
Connected to 192.168.5.1.
Escape character is '^]'.
AUTH ANONYMOUS
OK 4943a53752f52f82a9ea4e6e00000001
BEGIN
```

Vehicle on-board network

Automotive Cybersecurity

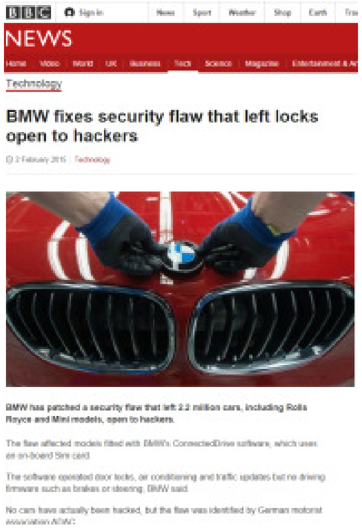
Recent issues

From **Wired** online *How Hackable Is Your Car?*

All the cars' ratings were based on an assessment made by two very famous hackers Charlie Miller and Chris Valasek. They defined three factors to evaluate "how a car Is hackable":

1. **size of their wireless "attack surface", features like Bluetooth, Wi-Fi, cellular network connections, keyless entry systems, and even radio-readable tire pressure monitoring systems.**
2. **vehicles' network architecture, how much access those possible footholds offered to more critical systems steering and brakes.**
3. **"cyberphysical" features: capabilities like automated braking, parking and lane assist that could transform a few spoofed digital commands into an actual out-of-control car.**

"Adventures in Automotive Networks and Control Units – by Dr. Charlie Miller & Chris Valasek"



BBC Sign in News Sport Weather Shop Earth Tra

NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Ar

Technology

BMW fixes security flaw that left locks open to hackers

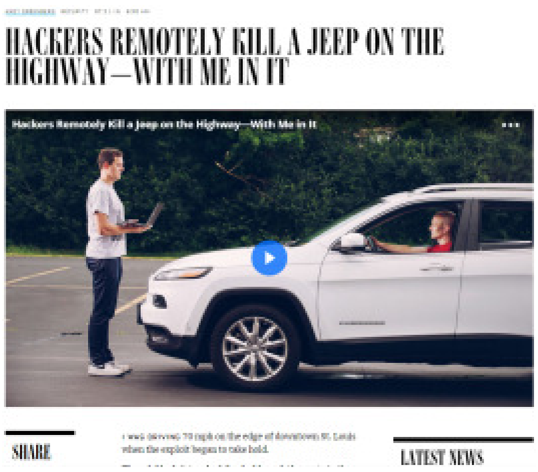
2 February 2015 | Technology

BMW has patched a security flaw that left 2.2 million cars, including Rolls Royce and Mini models, open to hackers.

The flaw affected models fitted with BMW's ConnectedDrive software, which uses an on-board Sim card.

The software operated door locks, air conditioning and traffic updates but no driving firmware such as brakes or steering, BMW said.

No cars have actually been hacked, but the flaw was identified by German motorist association ADAC.



ANDY GREENBERG SECURITY 07.21.15 6:00 AM

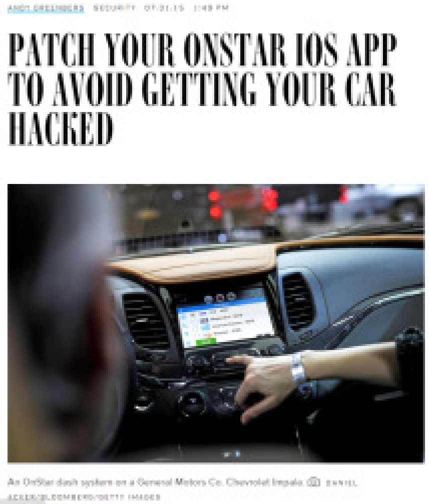
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me in It

SHARE

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

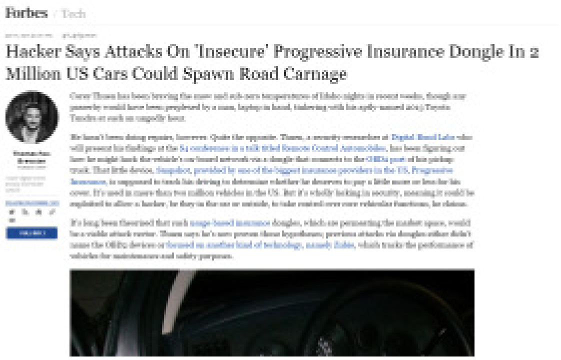
LATEST NEWS



ANDY GREENBERG SECURITY 07.31.15 1:49 PM

PATCH YOUR ONSTAR IOS APP TO AVOID GETTING YOUR CAR HACKED

An OnStar dash system on a General Motors Co. Chevrolet Impala. DANIEL ACKER/BLOOMBERG/GETTY IMAGES



Forbes / Tech

Hacker Says Attacks On 'Insecure' Progressive Insurance Dongle In 2 Million US Cars Could Spawn Road Carnage

Thomas Fox-Brewster

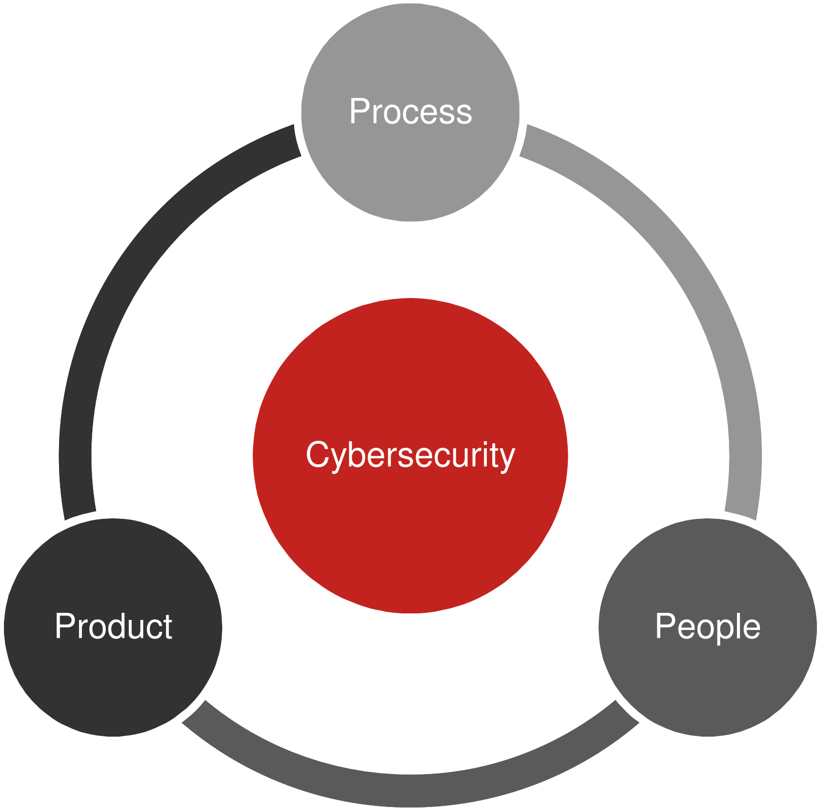
Corey Thuen has been braving the snow and sub-zero temperatures of Idaho nights in recent weeks, though any passerby would have been perplexed by a man, laptop in hand, tinkering with his aptly-named 2013 Toyota Tundra at such an ungodly hour.

He hasn't been doing repairs, however. Quite the opposite. Thuen, a security researcher at Digital Bond Labs who will present his findings at the S4 conference in a talk titled Remote Control Automobiles, has been figuring out how he might hack the vehicle's on-board network via a dongle that connects to the OBD2 port of his pickup truck. That little device, Snapshot, provided by one of the biggest insurance providers in the US, Progressive Insurance, is supposed to track his driving to determine whether he deserves to pay a little more or less for his cover. It's used in more than two million vehicles in the US. But it's wholly lacking in security, meaning it could be exploited to allow a hacker, be they in the car or outside, to take control over core vehicular functions, he claims.

It's long been theorised that such usage-based insurance dongles, which are permeating the market space, would be a viable attack vector. Thuen says he's now proven those hypotheses; previous attacks via dongles either didn't name the OBD2 devices or focused on another kind of technology, namely Zubie, which tracks the performance of vehicles for maintenance and safety purposes.

Automotive Cybersecurity

Possible impacts

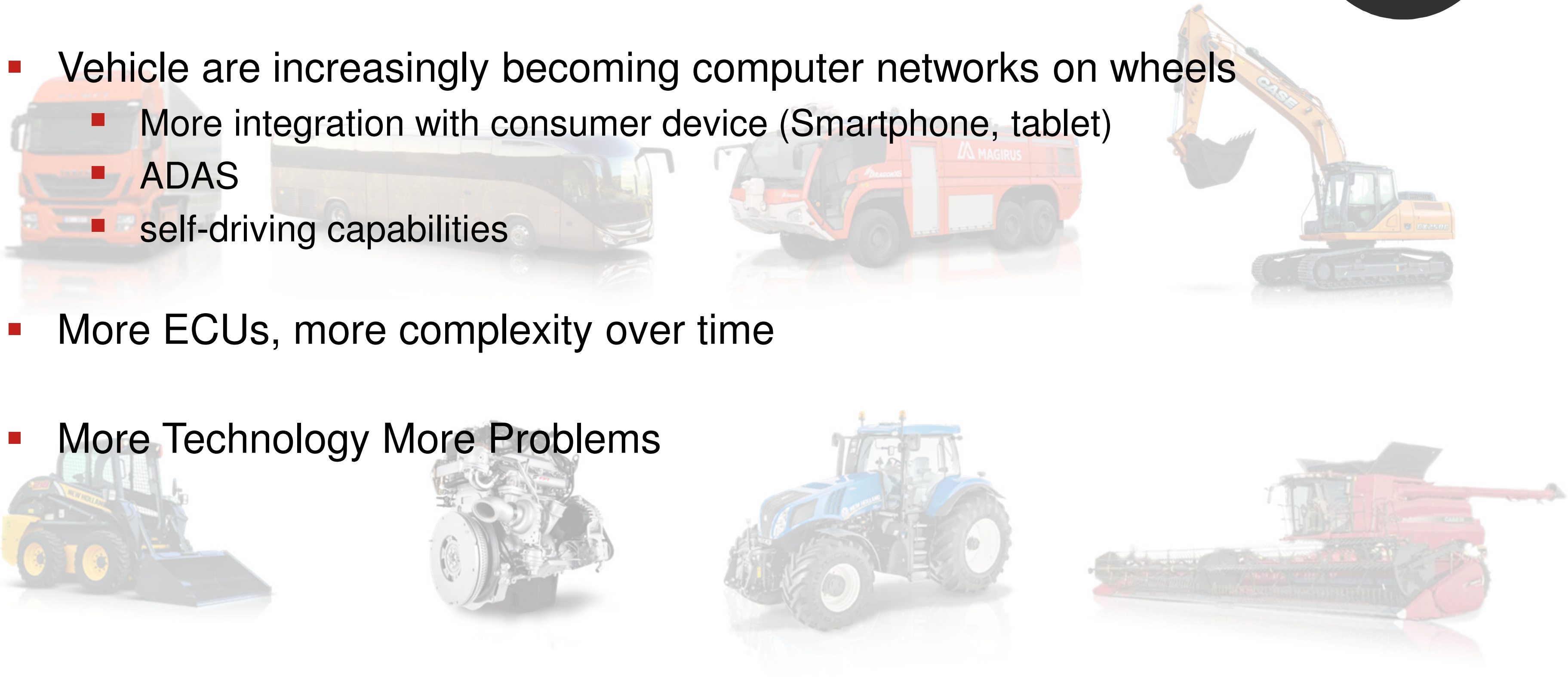


Automotive Cybersecurity

Possible impacts

Product

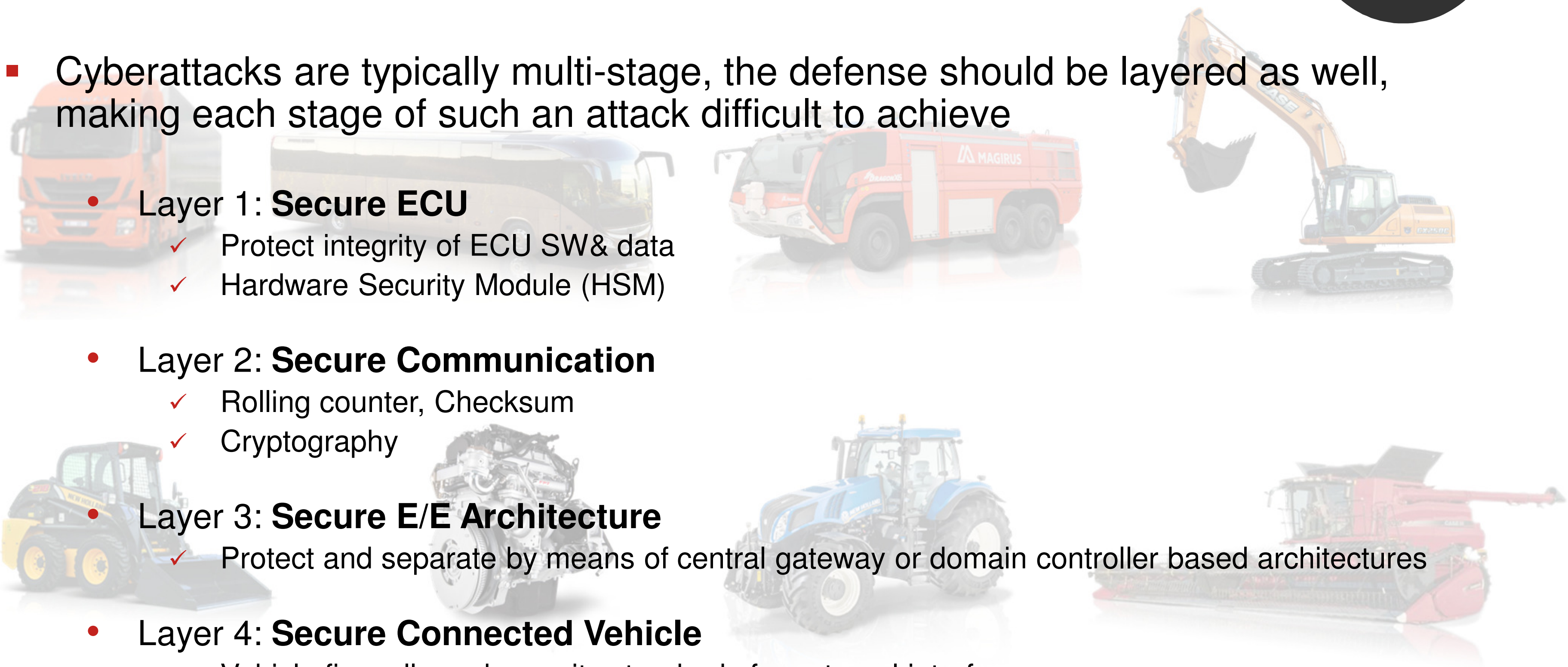
- Vehicle are increasingly becoming computer networks on wheels
  - More integration with consumer device (Smartphone, tablet)
  - ADAS
  - self-driving capabilities
- More ECUs, more complexity over time
- More Technology More Problems



Automotive Cybersecurity

Possible impacts

Product



- Cyberattacks are typically multi-stage, the defense should be layered as well, making each stage of such an attack difficult to achieve
  - Layer 1: **Secure ECU**
    - ✓ Protect integrity of ECU SW& data
    - ✓ Hardware Security Module (HSM)
  - Layer 2: **Secure Communication**
    - ✓ Rolling counter, Checksum
    - ✓ Cryptography
  - Layer 3: **Secure E/E Architecture**
    - ✓ Protect and separate by means of central gateway or domain controller based architectures
  - Layer 4: **Secure Connected Vehicle**
    - ✓ Vehicle firewalls and security standards for external interfaces

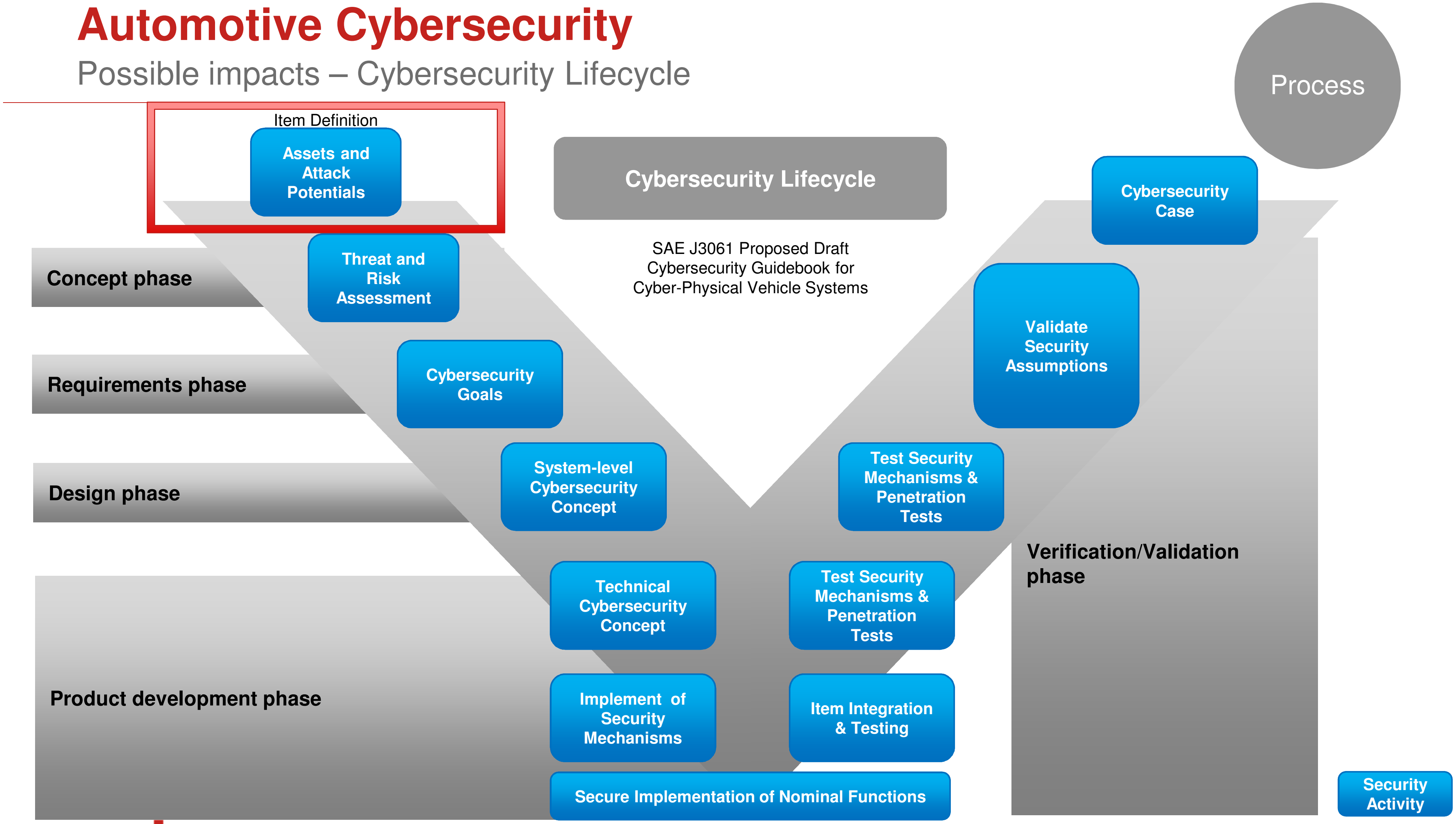
Automotive Cybersecurity

Possible impacts – Cybersecurity Lifecycle

- Cybersecurity must be built in to the design rather than added on at the end of development
- Building cybersecurity into the design requires an appropriate lifecycle process from the concept phase through production, operation, and service
- SAE J3061 (Draft Proposal) provides a framework process

Automotive Cybersecurity

Possible impacts – Cybersecurity Lifecycle


Process
Item Definition
Assets and Attack Potentials
Cybersecurity Lifecycle
Cybersecurity Case
Concept phase
Threat and Risk Assessment
Requirements phase
Cybersecurity Goals
Validate Security Assumptions
Design phase
System-level Cybersecurity Concept
Test Security Mechanisms & Penetration Tests
Verification/Validation phase
Technical Cybersecurity Concept
Test Security Mechanisms & Penetration Tests
Product development phase
Implement of Security Mechanisms
Item Integration & Testing
Secure Implementation of Nominal Functions
Security Activity

SAE J3061 Proposed Draft
Cybersecurity Guidebook for
Cyber-Physical Vehicle Systems

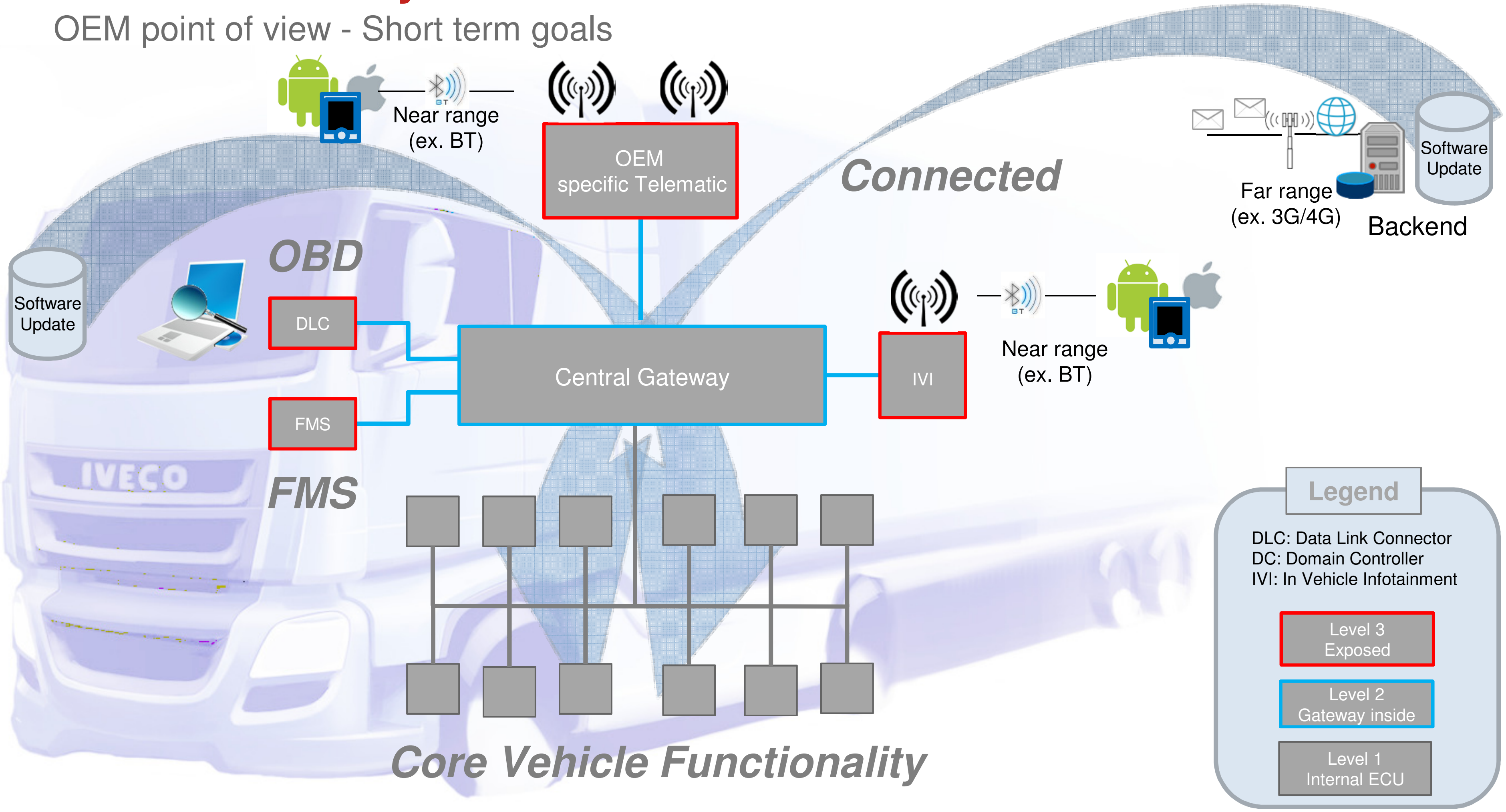
Automotive Cybersecurity

OEM point of view - Description of main drivers

- The near future will see automated and **autonomous vehicles** and connected and cooperative driving
- The new developments will have a **great impact on society**
- **Vehicles become more automated**
- These developments increasingly **connect the infrastructure, the driver and the vehicle**
- On this scenario the Cybersecurity will be a key aspect
- Vehicles have been designed with safety in mind.
  However, we cannot have safety without security

Central Gateway based Architecture

OEM point of view - Short term goals



Legend

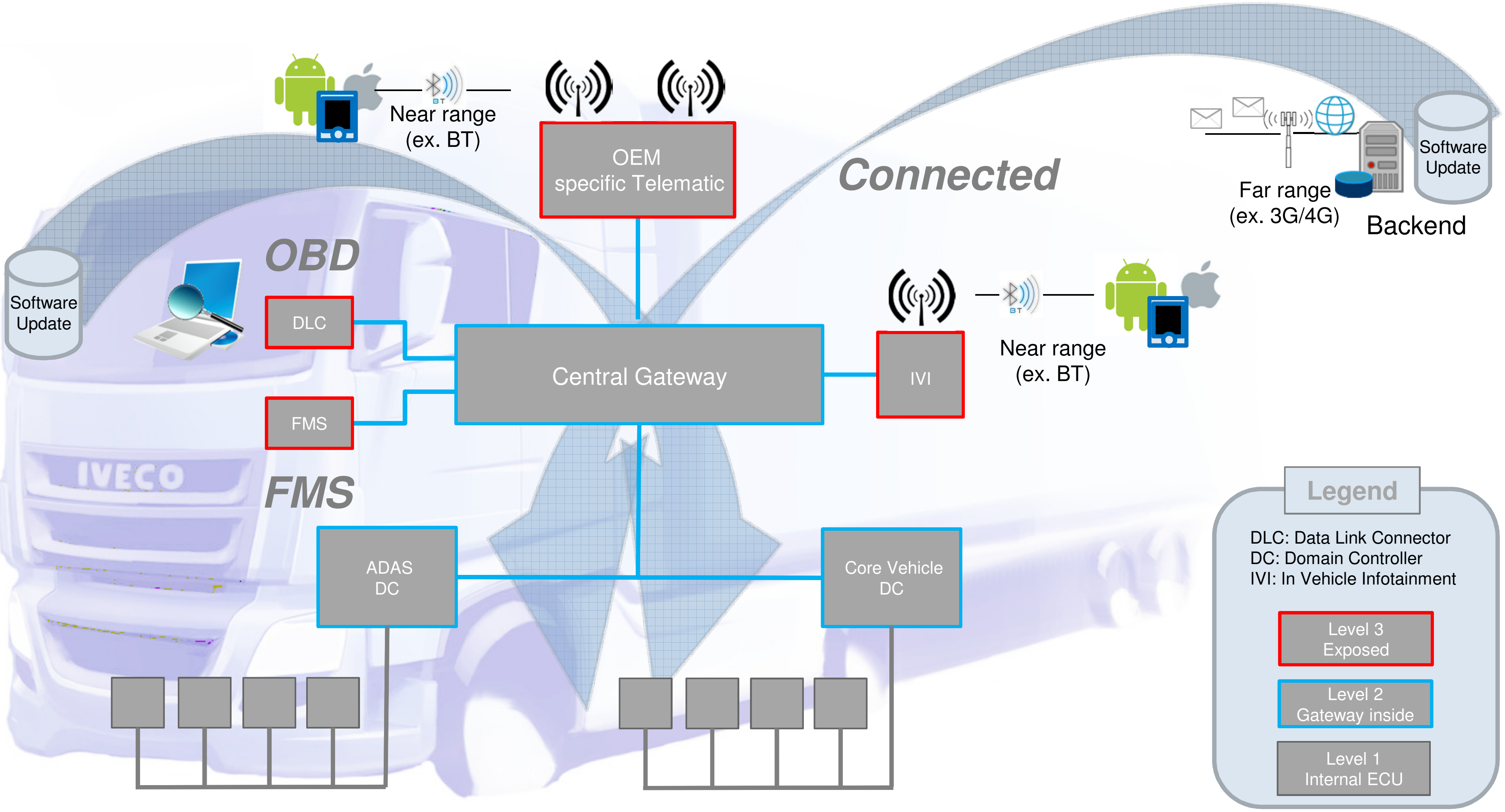
DLC: Data Link Connector
DC: Domain Controller
IVI: In Vehicle Infotainment

🟥 Level 3
Exposed

🟦 Level 2
Gateway inside

Level 1
Internal ECU

Domain Controller based Architecture



Legend

DLC: Data Link Connector
DC: Domain Controller
IVI: In Vehicle Infotainment

🟥 Level 3 Exposed

🟦 Level 2 Gateway inside

Level 1 Internal ECU

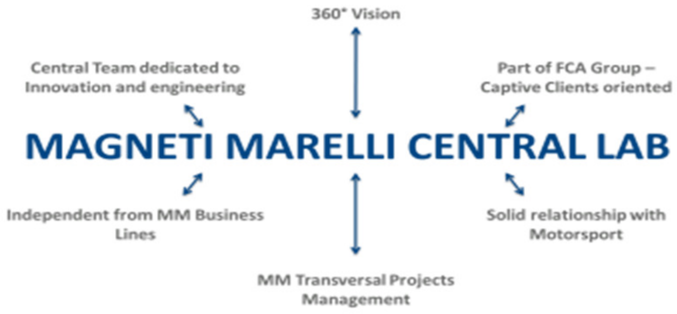
Automotive Cybersecurity

Magneti Marelli approach

Our vision is that we cannot be a Leading Actor in the Automotive Market without Secured Products

A team dedicated to Cybersecurity integrated in the MM Central Lab

- Offering Cybersecurity Engineering services in terms of
  - Vehicle Vulnerability Assessments and Penetration Tests
  - Identification of HW solutions and architecture refinement
  - Security SW stack ready for integration
- Supporting the MM BLs and captive customers in the definition of Cybersecurity requirements



360° Vision

Central Team dedicated to Innovation and engineering

Part of FCA Group – Captive Clients oriented

MAGNETI MARELLI CENTRAL LAB

Independent from MM Business Lines

Solid relationship with Motorsport

MM Transversal Projects Management

Automotive Cybersecurity

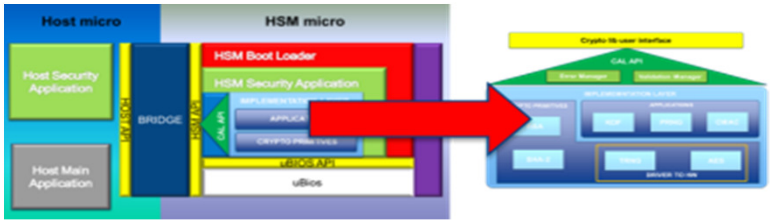
Magneti Marelli Cyber Security Lab – On-going activities

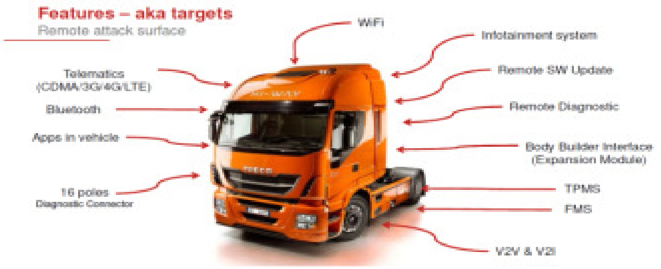
MM Cybersecurity Lab
An engineering center oriented to Cybersecurity applications

- Availability of Automotive Cyber Security SW stack
- Vehicle Penetration Tests
- Simulation of Cyber Security requirements
- Development of Cyber Security IPs

Development of **Cryptographic SW library** for automotive applications

- First application on Engine Management ECU for German OEM





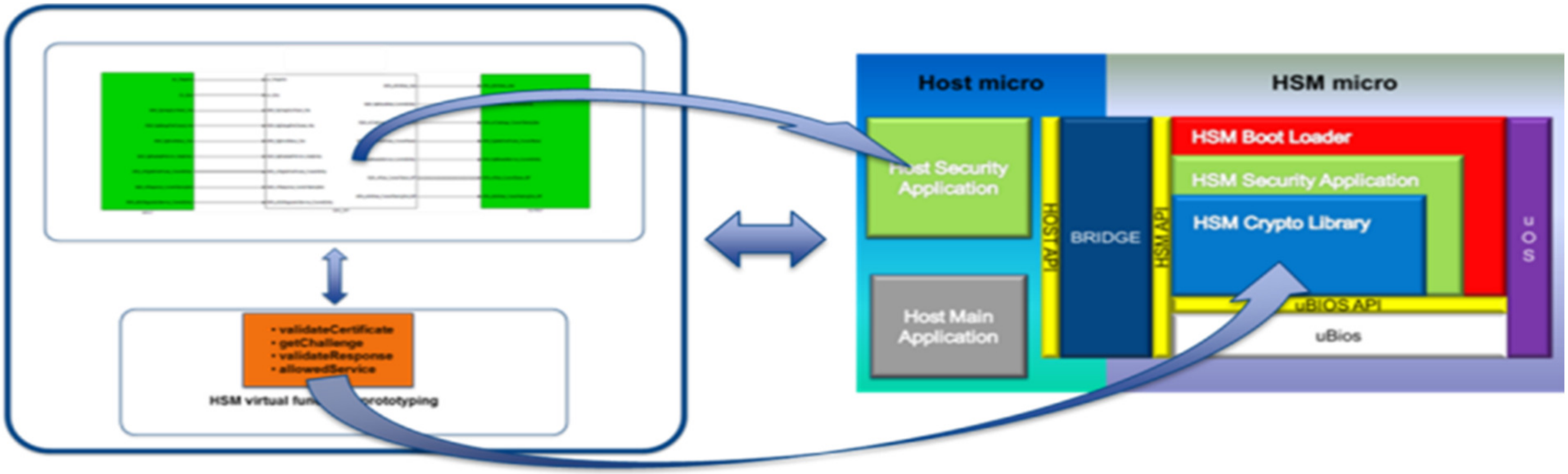
IVECO Cyber Security road map

- Vulnerability assessment of future vehicle EE architecture of Heavy Duty truck
- Identification of a mitigation road map including impacts on EE architecture, HW and SW

Automotive Cybersecurity

Magneti Marelli Cyber Security Lab – Cyber Security Rapid Prototyping

- Simulink modeling of Cyber Security system requirements and automatic code generation
- Virtualization of selected Hardware Trust Anchors based on Virtual Prototyping Environments
- System pre-assessment by integration of modeled requirements in vehicle simulator



Automotive Cybersecurity

Conclusion

- More and more technology is being added every year, creating additional attack surface
- More connectivity requires more security
- It is necessary to move the Focus on a new paradigm: the **Extended Vehicle**
- Collaboration is needed between the following stakeholders:
  OEM, suppliers, mobile telecommunications, ICT companies
- Cybersecurity is a continuous process, through the following main principles
  - Identify
  - Protect
  - Detect
  - Response
  - Recover

Contacts

EHSA – SSCA System Integration
System Architecture
alessandro.farsaci@cnhind.com

www.cnhindustrial.com

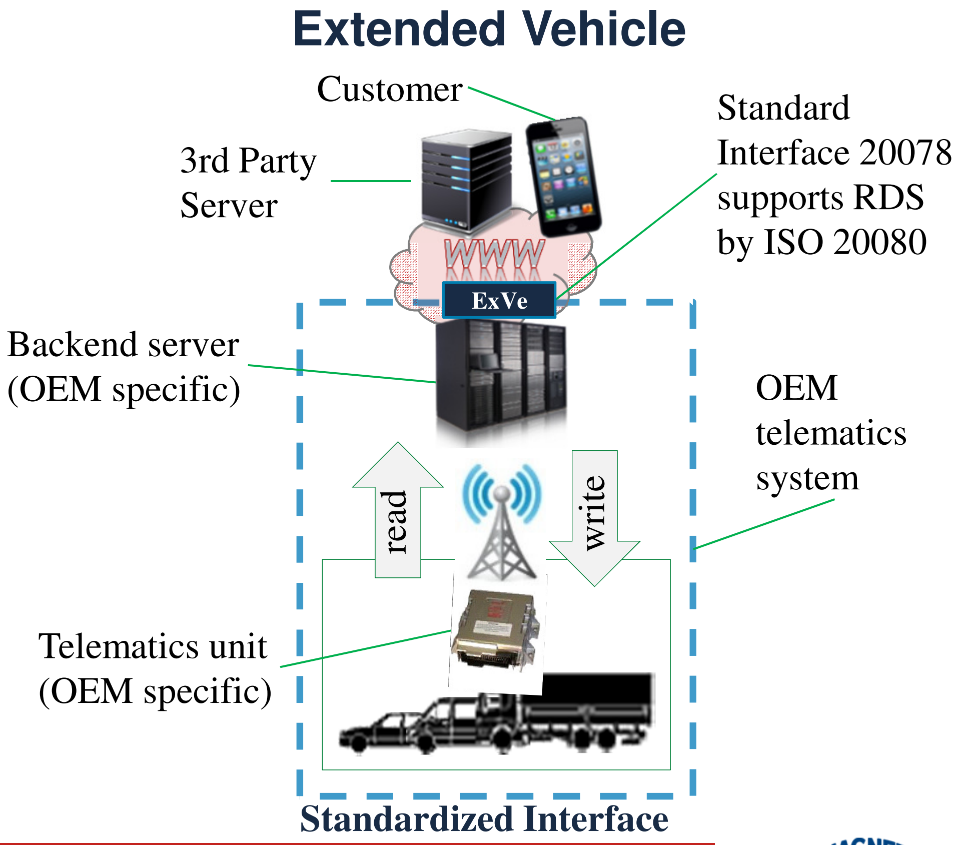
System and SW Engineering Center
Automotive Cybersecurity Program Manager
cosimo.senni@magnetimarelli.com

www.magnetimarelli.com

Backup

The Open Platform – Extended Vehicle (ExVe) as the single Solution for Remote Diagnostics Support (RDS)

The Extended Vehicle (ExVe) provides by the new ISO standardization project no. 20078 the technical solution for the Remote Diagnostics Support (RDS), which is supported by the new ISO standardization project no. 20080.


Extended Vehicle
Customer
3rd Party Server
Standard Interface 20078 supports RDS by ISO 20080
WWW
ExVe
Backend server (OEM specific)
OEM telematics system
read
write
Telematics unit (OEM specific)
Standardized Interface

News from ACEA

JC paper on automation (JC//15)

ACEA European Automobile Manufacturers Association

- The JC is requested to approve the following changes to the ACEA organisation:
  - Give WG-CONNECT overall responsibility for policy issues related to automation
  - **Set up a task force cybersecurity reporting to WG-CONNECT**
- Status
  The issue of motor vehicle automation is attracting increasing attention from policy makers:
  - The Vienna Convention has been modified to <u>enable motor vehicle driving on public roads without the driver</u> being in control of the vehicle at all times and further modifications are being envisaged
  - The UN ECE Regulation 79 on steering is being modified <u>to permit automated steering functions at higher speeds</u>
  - The UN ECE has set up three informal groups on automated driving
  - The Dutch Presidency will set up a dialogue between governments and industry on connected and automated driving
  - Several Member States have adopted policy papers on automated driving and <u>are permitting testing on public roads</u>
  - The EU is making available funding for field operational tests within Horizon 2020
  - The European Commission (DG GROW) intends to make automated driving one of its focus areas within the GEAR 2030 programme
  - Euro NCAP is looking into the possibility of <u>establishing tests and protocols for vehicles with automated functions</u>
  - The mandatory installation of an event data recorder in motor vehicles is being contemplated as a means to address liability questions

News from ACEA

CONNECTIVITY STRATEGY PAPER

European Automobile Manufacturers Association

- Data is the basis for Connectivity
  - Giving any third party unlimited and uncontrolled access to vehicle data would create serious issues of personal data protection, security, safety, liability and competition. These issues need to be addressed urgently.

- No Data access without Security, Safety and Liability
  - Share information about the latest security threats and possible countermeasures between vehicle manufacturers, suppliers, mobile telecommunications operators and possibly ICT companies (like Information Sharing and Analysis Centre ISAC in the United States)
  - The security of this information could no longer be assured if vehicle systems were open to third parties without restriction or control.
  - For this reason, third-party applications that interact with the vehicle should only be developed and approved in cooperation with the vehicle manufacturer to eliminate security, data protection and product liability risks.
  - This will also facilitate the work of regulatory and supervisory authorities, insurance companies and infrastructure managers who will continue to deal with a single central partner – the vehicle manufacturer – on approval-related and data protection matters, instead of with a large number of different service providers, many of whom are based outside the EU.

News from ACEA

CONNECTIVITY STRATEGY PAPER

European Automobile Manufacturers Association

- The exVeh provides the best technical solution
  - The extended vehicle offers open access interfaces for the provision of services by vehicle manufacturers or third parties.
    - ✓ The on-board diagnostics (OBD) interface for emission control and legally prescribed diagnostic services
    - ✓ The fleet management systems (FMS) interface for heavy duty vehicles (based on the industry standard)
    - ✓ A web interface: for example, for remote diagnostic support (RDS) and for remote fleet management systems (rFMS) for heavy duty vehicles (based on the industry standard)
  - Extended vehicle advantages:
    - ✓ OEM controls and secures all data transmission channels
    - ✓ emergency intervention by OTA (If a new system security risk emerges)
    - ✓ Standardised provision of vehicle data minimises development effort for third parties
    - ✓ Providers selected and authorised by the customer are granted read access to specific vehicle data. Interfaces are designed to exclude write access to vehicle data
    - ✓ Legal data protection controlled by customers themselves
    - ✓ Customer consent is the basis for all data-based value-added services