# Development of Intrusion Detection System for vehicle CAN bus cyber security

Anastasia Cornelio, Elisa Bragaglia, Cosimo Senni, Walter Nesci

Technology Innovation - SSEC

14° Workshop Automotive SPIN Italia

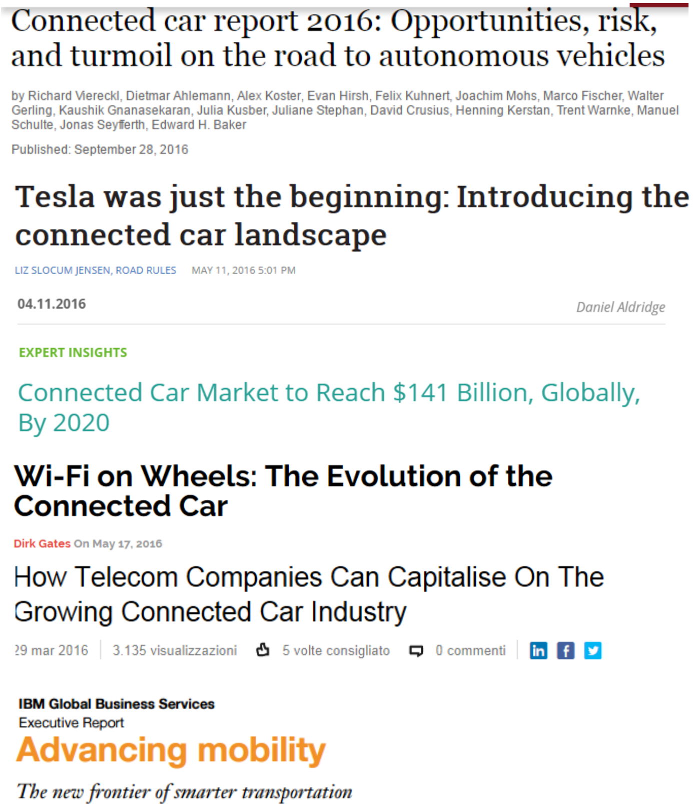
November 10th, 2016

# Index

- Introduction
- The Threat of Dongles
- Cyber Attacks
  - Cause an accident
  - Damage company’s image
  - Cause a financial loss
- Intrusion Detection System
- Security improvement
- Vehicle Recovery System

# Introduction: Connected vehicles

**2016 saw the explosion of technologies and research for connected vehicles.**



Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles

by Richard Viereckl, Dietmar Ahlemann, Alex Koster, Evan Hirsh, Felix Kuhnert, Joachim Mohs, Marco Fischer, Walter Gerling, Kaushik Gnanasekaran, Julia Kusber, Juliane Stephan, David Crusius, Henning Kerstan, Trent Warnke, Manuel Schulte, Jonas Seyfferth, Edward H. Baker

Published: September 28, 2016

Tesla was just the beginning: Introducing the connected car landscape

LIZ SLOCUM JENSEN, ROAD RULES MAY 11, 2016 5:01 PM

04.11.2016 Daniel Aldridge

EXPERT INSIGHTS

Connected Car Market to Reach $141 Billion, Globally, By 2020

Wi-Fi on Wheels: The Evolution of the Connected Car

Dirk Gates On May 17, 2016

How Telecom Companies Can Capitalise On The Growing Connected Car Industry

29 mar 2016 | 3.135 visualizzazioni | 5 volte consigliato | 0 commenti

IBM Global Business Services

Executive Report

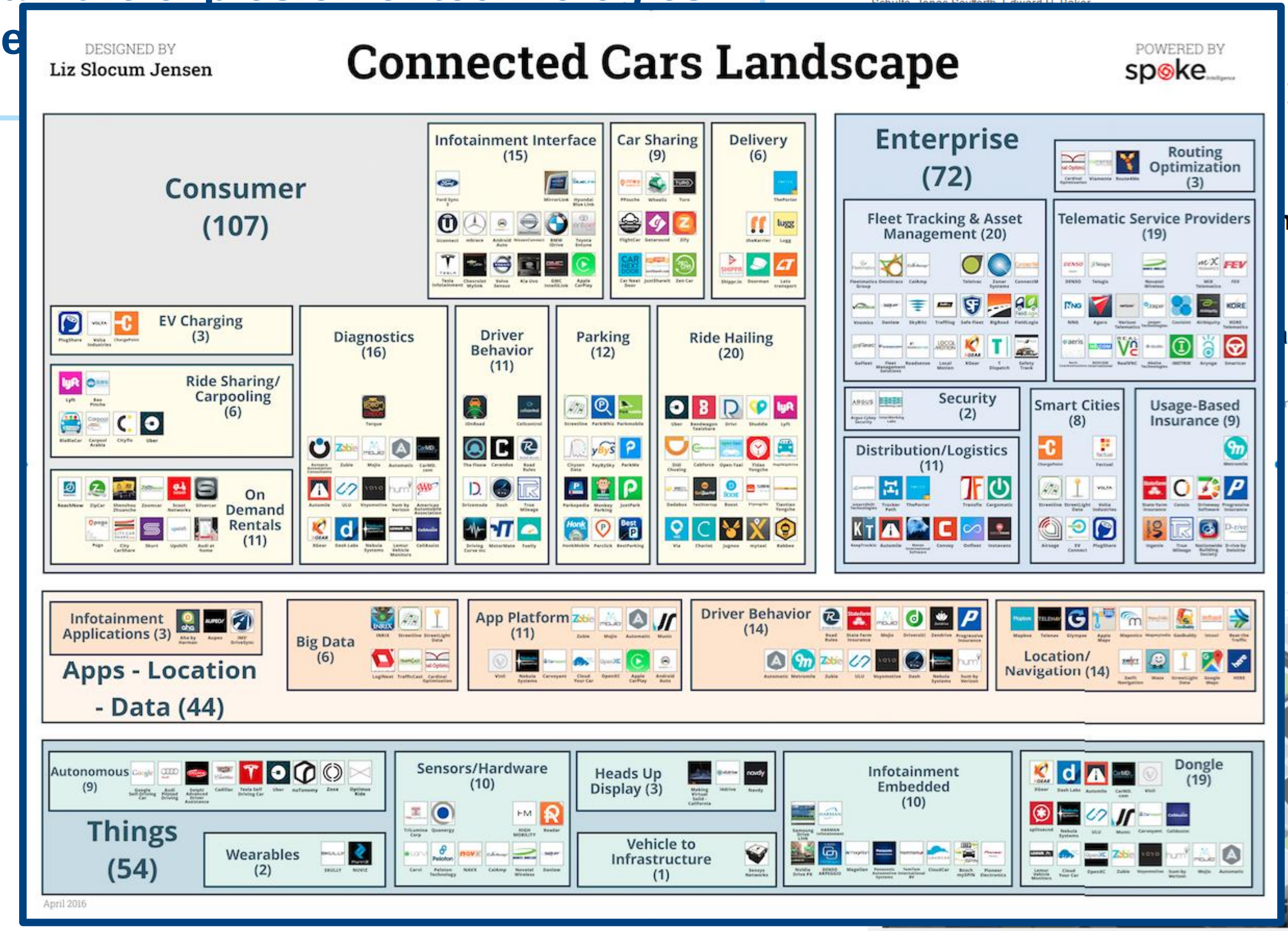
Advancing mobility

*The new frontier of smarter transportation*

Shaping the Future of Urban Mobility with the Connected Vehicle

# Introduction: Connected vehicles

2016 saw the explosion of technologies
and re



Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles

by Richard Viereckl, Dietmar Ahlemann, Alex Koster, Evan Hirsh, Felix Kuhnert, Joachim Mohs, Marco Fischer, Walter Gerling, Kaushik Gnanasekaran, Julia Kusber, Juliane Stephan, David Crusius, Henning Kerstan, Trent Warnke, Manuel Schulte, Jonas Seyfarth, Edward H. Baker

Introducing the

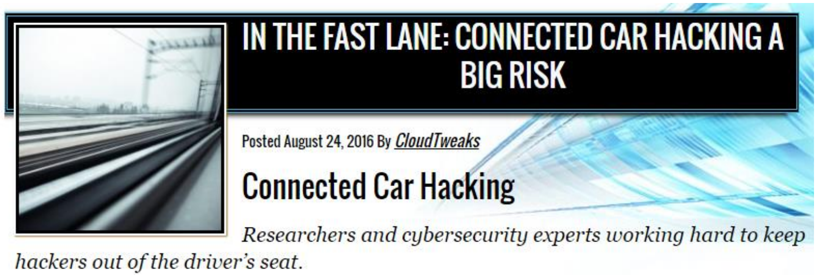
of the

lise On The

mmenti

Shaping the Future of Urban Mobility with the Connected Vehicle

# Introduction: The big risk

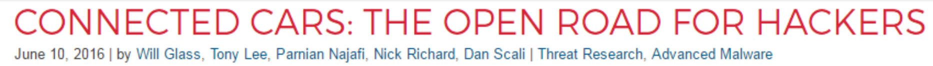


IN THE FAST LANE: CONNECTED CAR HACKING A BIG RISK

Posted August 24, 2016 By CloudTweaks

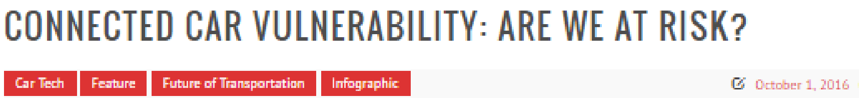
Connected Car Hacking

*Researchers and cybersecurity experts working hard to keep hackers out of the driver's seat.*



CONNECTED CARS: THE OPEN ROAD FOR HACKERS

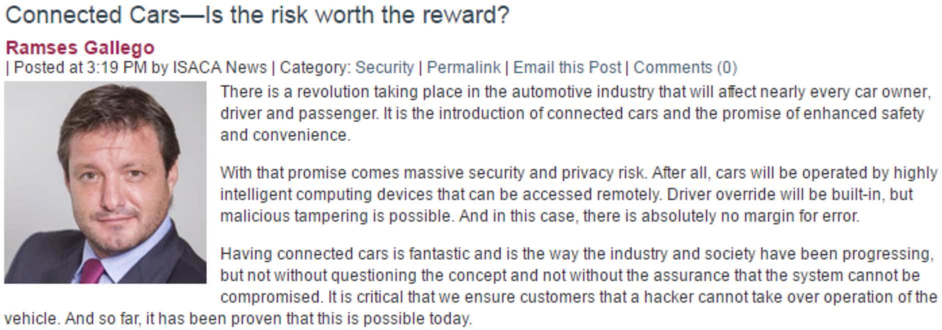
June 10, 2016 | by Will Glass, Tony Lee, Parnian Najafi, Nick Richard, Dan Scali | Threat Research, Advanced Malware



CONNECTED CAR VULNERABILITY: ARE WE AT RISK?

Car Tech | Feature | Future of Transportation | Infographic

October 1, 2016



Connected Cars—Is the risk worth the reward?

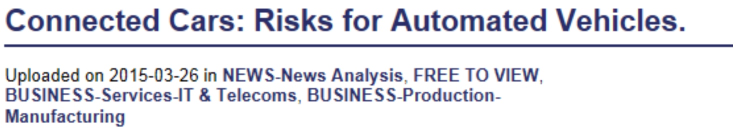
Ramses Gallego

| Posted at 3:19 PM by ISACA News | Category: Security | Permalink | Email this Post | Comments (0)

There is a revolution taking place in the automotive industry that will affect nearly every car owner, driver and passenger. It is the introduction of connected cars and the promise of enhanced safety and convenience.

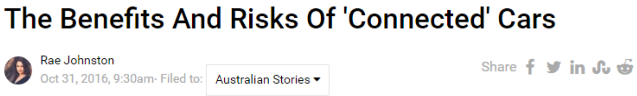
With that promise comes massive security and privacy risk. After all, cars will be operated by highly intelligent computing devices that can be accessed remotely. Driver override will be built-in, but malicious tampering is possible. And in this case, there is absolutely no margin for error.

Having connected cars is fantastic and is the way the industry and society have been progressing, but not without questioning the concept and not without the assurance that the system cannot be compromised. It is critical that we ensure customers that a hacker cannot take over operation of the vehicle. And so far, it has been proven that this is possible today.



Connected Cars: Risks for Automated Vehicles.

Uploaded on 2015-03-26 in NEWS-News Analysis, FREE TO VIEW, BUSINESS-Services-IT & Telecoms, BUSINESS-Production-Manufacturing

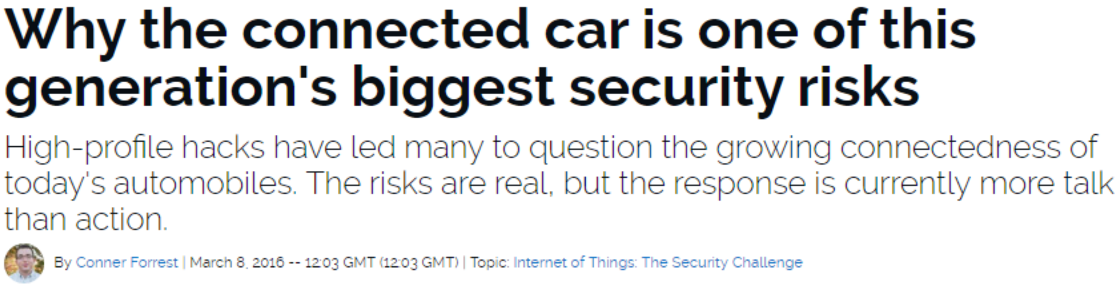


The Benefits And Risks Of 'Connected' Cars

Rae Johnston

Oct 31, 2016, 9:30am · Filed to: Australian Stories ▾

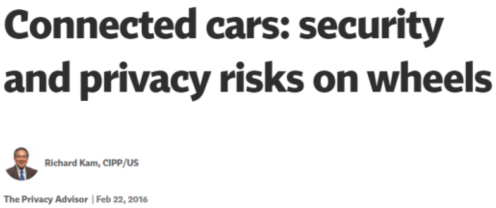
Share



Why the connected car is one of this generation's biggest security risks

High-profile hacks have led many to question the growing connectedness of today's automobiles. The risks are real, but the response is currently more talk than action.

By Conner Forrest | March 8, 2016 -- 12:03 GMT (12:03 GMT) | Topic: Internet of Things: The Security Challenge



Connected cars: security and privacy risks on wheels

Richard Kam, CIPP/US

The Privacy Advisor | Feb 22, 2016

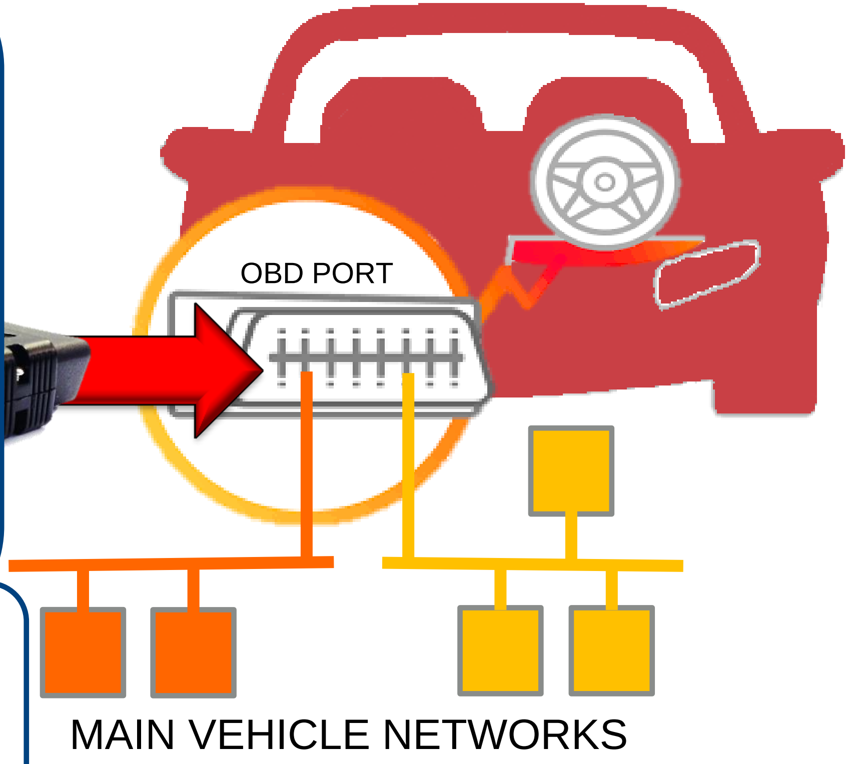
# The threat of Dongles

## Also not connected vehicles are subject to the same risk

On-Board Diagnostics (OBD) ports, used for diagnostic purposes, are present on every vehicle.

Main CAN networks are exposed on OBD port, mapped following the SAE J1962 standard port.

They are cheap devices associated also to apps via Wi-Fi or Bluetooth

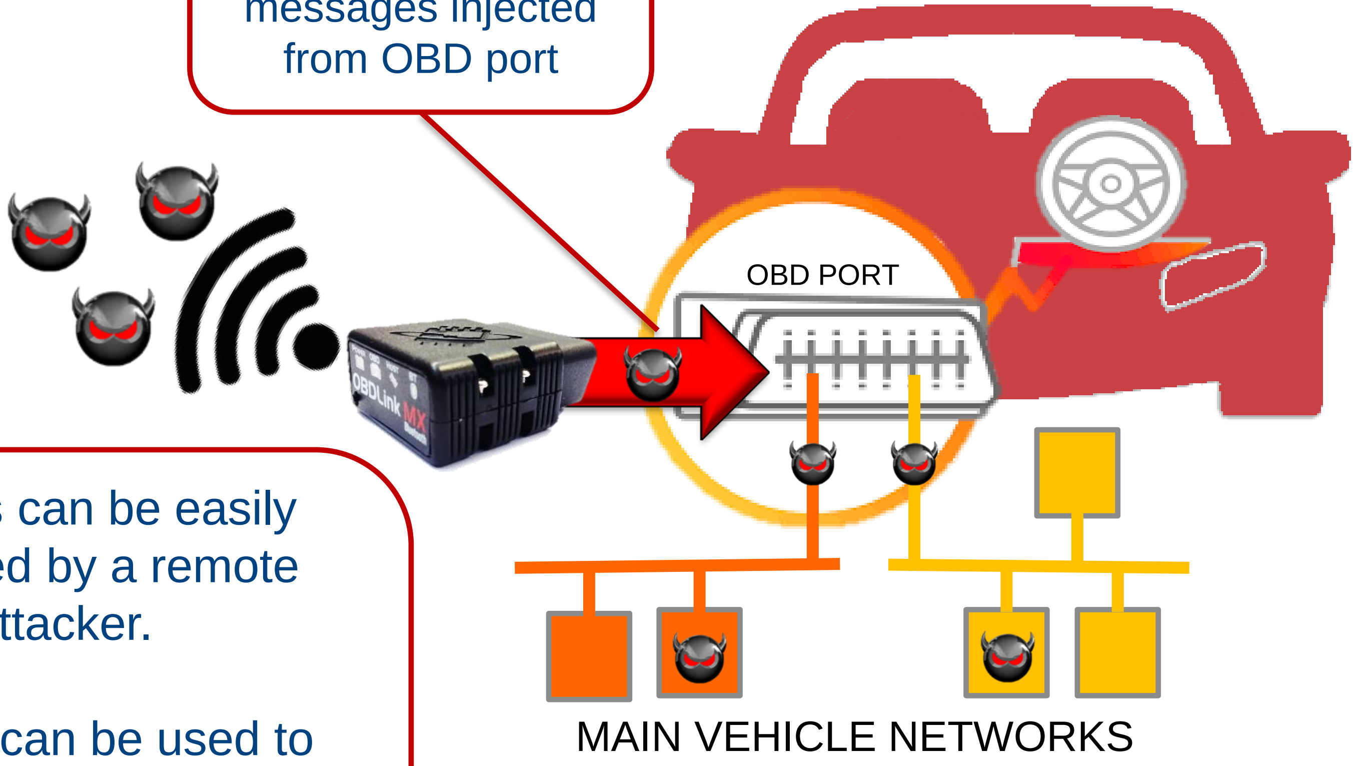


They are used by consumers but also from **insurance companies** to monitor vehicle’s state (e.g. speed, ECUs faults)

# The threat of Dongles

**Also not connecte** **ct to the same risks**

No special controls are applied on messages injected from OBD port



Dongles can be easily controlled by a remote attacker.

Dongles can be used to sniff all vehicle communication and to inject dangerous messages in vehicle network.

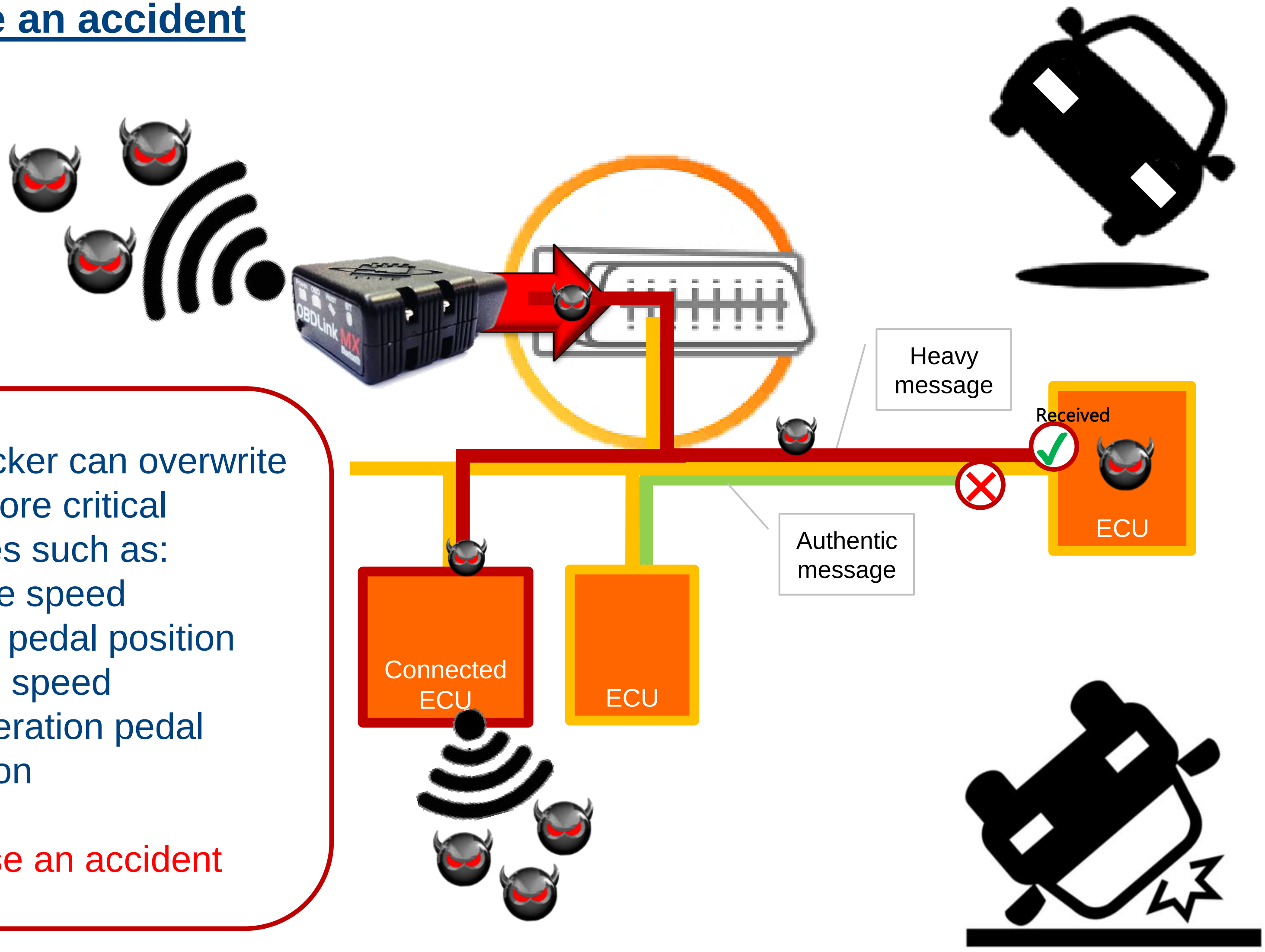
# Cyber Attacks I

## Cause an accident

The attacker can overwrite one or more critical messages such as:

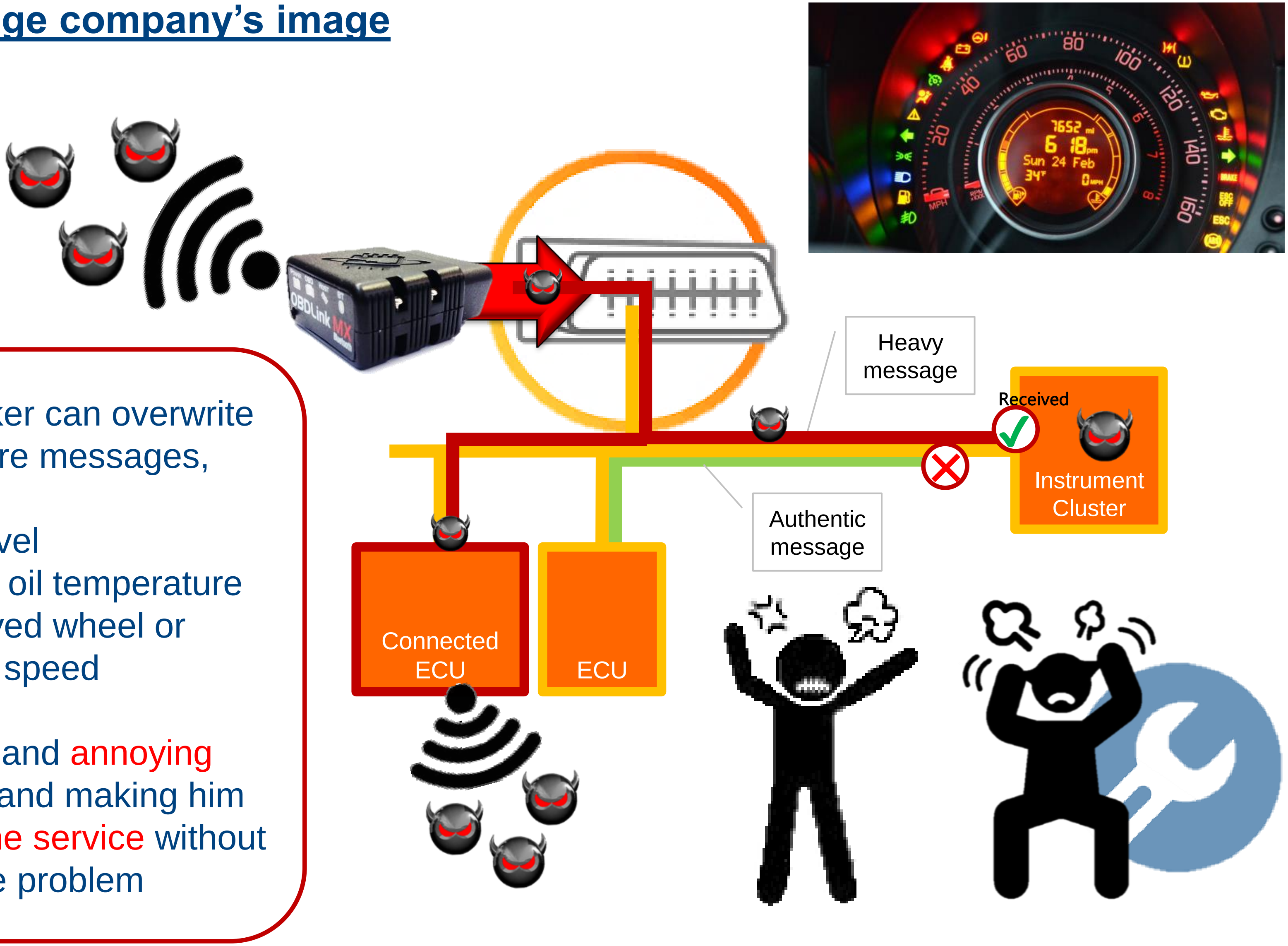
- engine speed
- brake pedal position
- wheel speed
- acceleration pedal position

and cause an accident



# Cyber Attacks II

## Damage company’s image



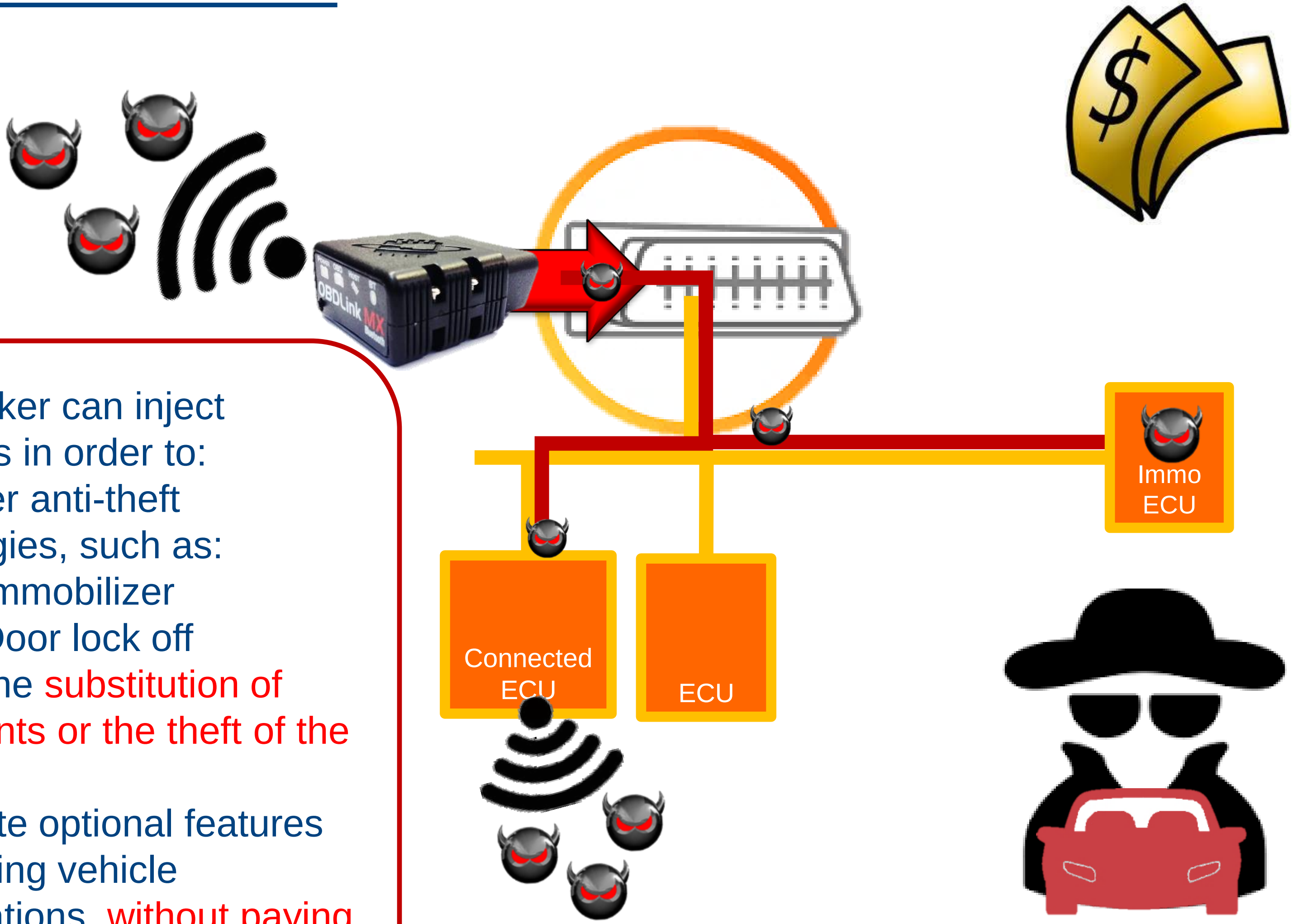
The attacker can overwrite one or more messages, such as:

- Fuel level
- Engine oil temperature
- Displayed wheel or engine speed

disturbing and annoying the driver and making him going to the service without solving the problem

# Cyber Attacks III

## Cause a financial loss



The attacker can inject messages in order to:

- ○ Tamper anti-theft strategies, such as:
  - Immobilizer
  - Door lock off

causing the substitution of components or the theft of the vehicle

- ○ Activate optional features changing vehicle calibrations, without paying for them

# Security solutions

## 1. OBD port firewall

A firewall is a device to be mounted behind the OBD port aimed to:

- monitor the incoming CAN frames
- filter out the invalid packets

PATENT PENDING n. 102016000109368

## 2. Intrusion Detection System (IDS)

An IDS is a set of SW and/or HW components aimed to:

- monitor the traffic of a network
- raise an alert in case of malicious activities or policy violations
- record the identified intrusions

- **Different roles in security**

**Firewall**

Lock to the gates

**IDS**

Video surveillance system

# IDS: how does it work?

- **Anomaly-based detection techniques**

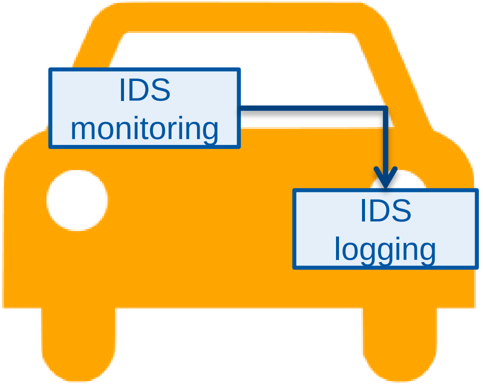
### training

a preliminary **learning phase** is required in order to define the reference normal CAN traffic behavior

### execution

while monitoring the CAN traffic, the current state is compared with the previously learned one

- **Main tasks**



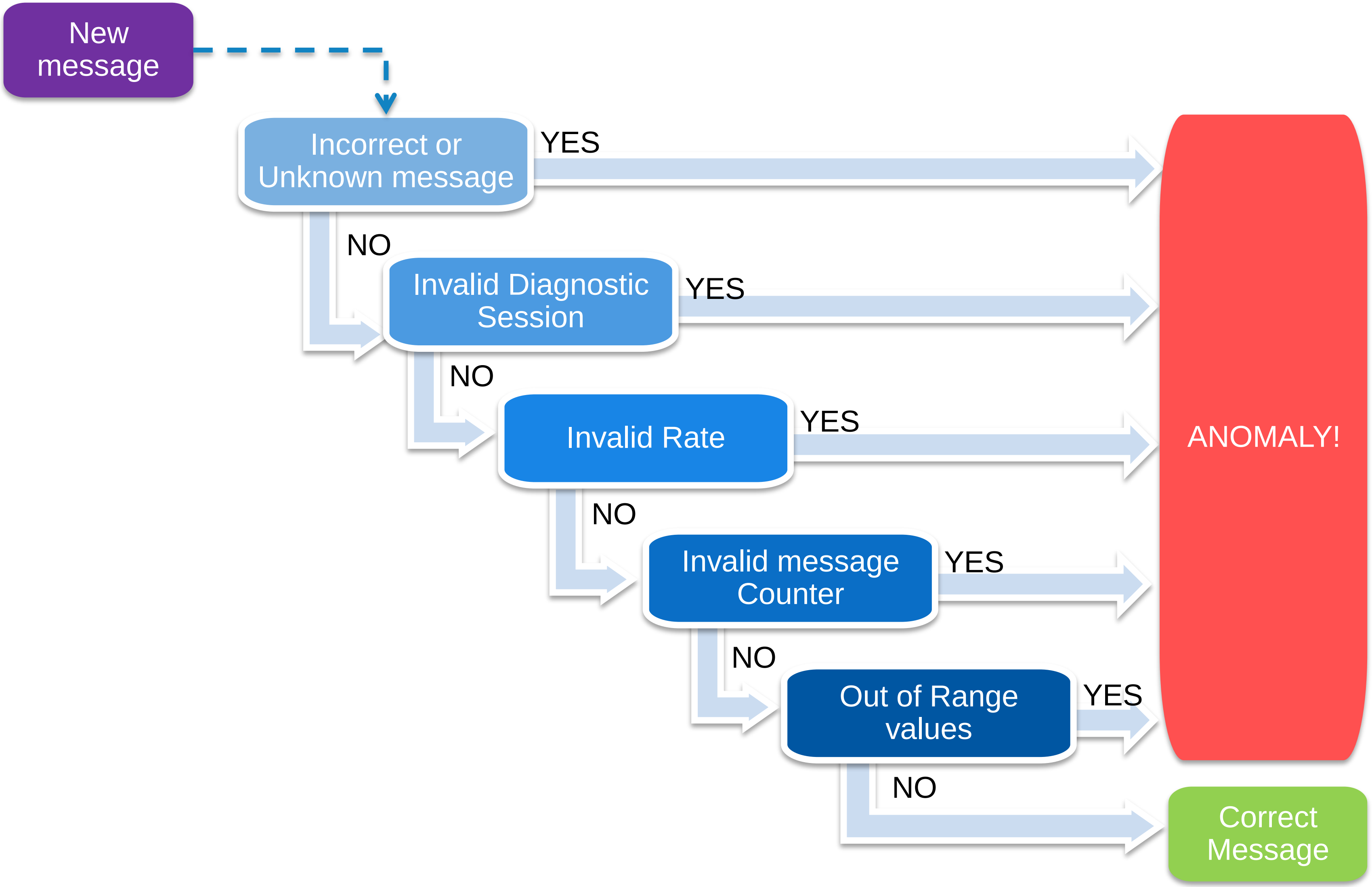
IDS monitoring

IDS logging

- Check of each CAN frame
- Logging of identified intrusions

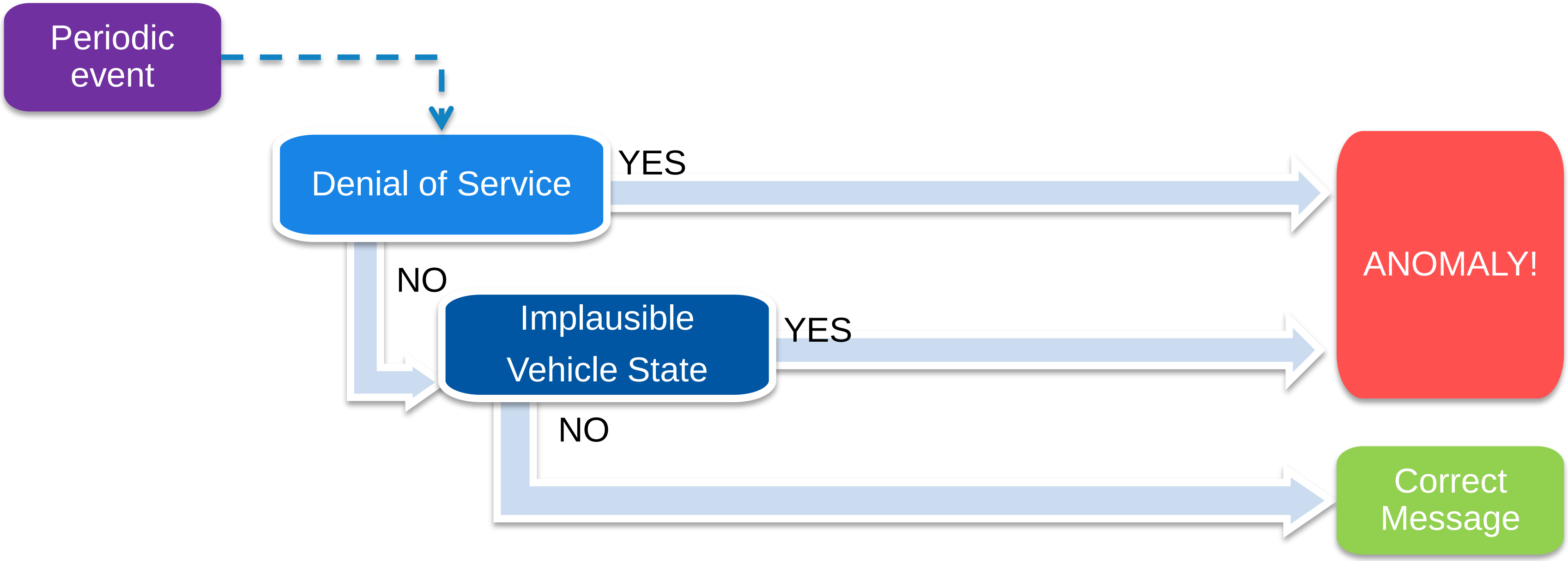
# IDS: how is it implemented?

- **A sequential check triggered by each new CAN frame**



# IDS: how is it implemented?

- **A sequential check triggered by periodic event**



Periodic event

Denial of Service

YES

NO

Implausible Vehicle State

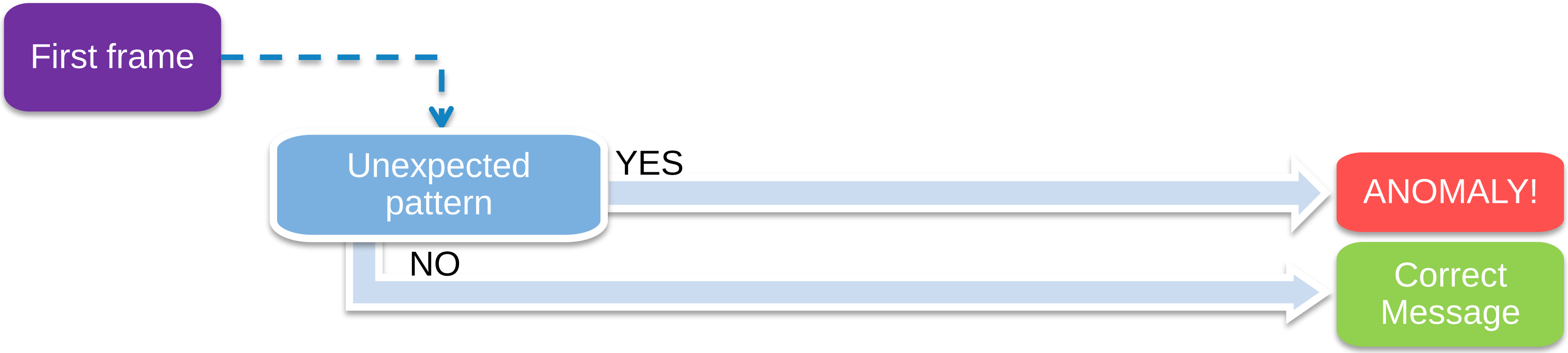
YES

NO

ANOMALY!

Correct Message

- **Check of special patterns triggered by one or more CAN frames**



First frame

Unexpected pattern

YES

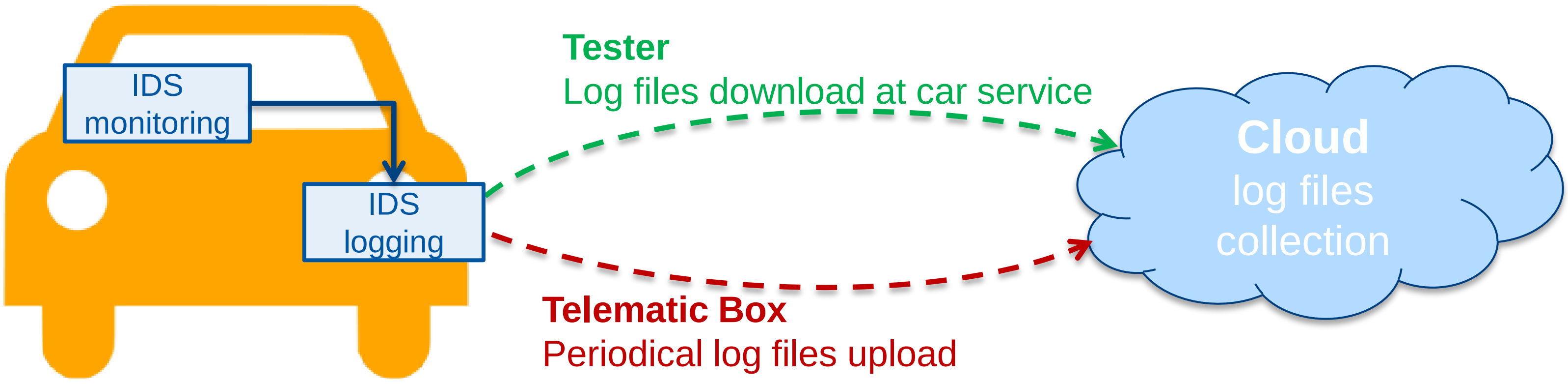
NO

ANOMALY!

Correct Message

# IDS: why is it useful?

- **Log can be analyzed by OEM**



**Tester**
Log files download at car service

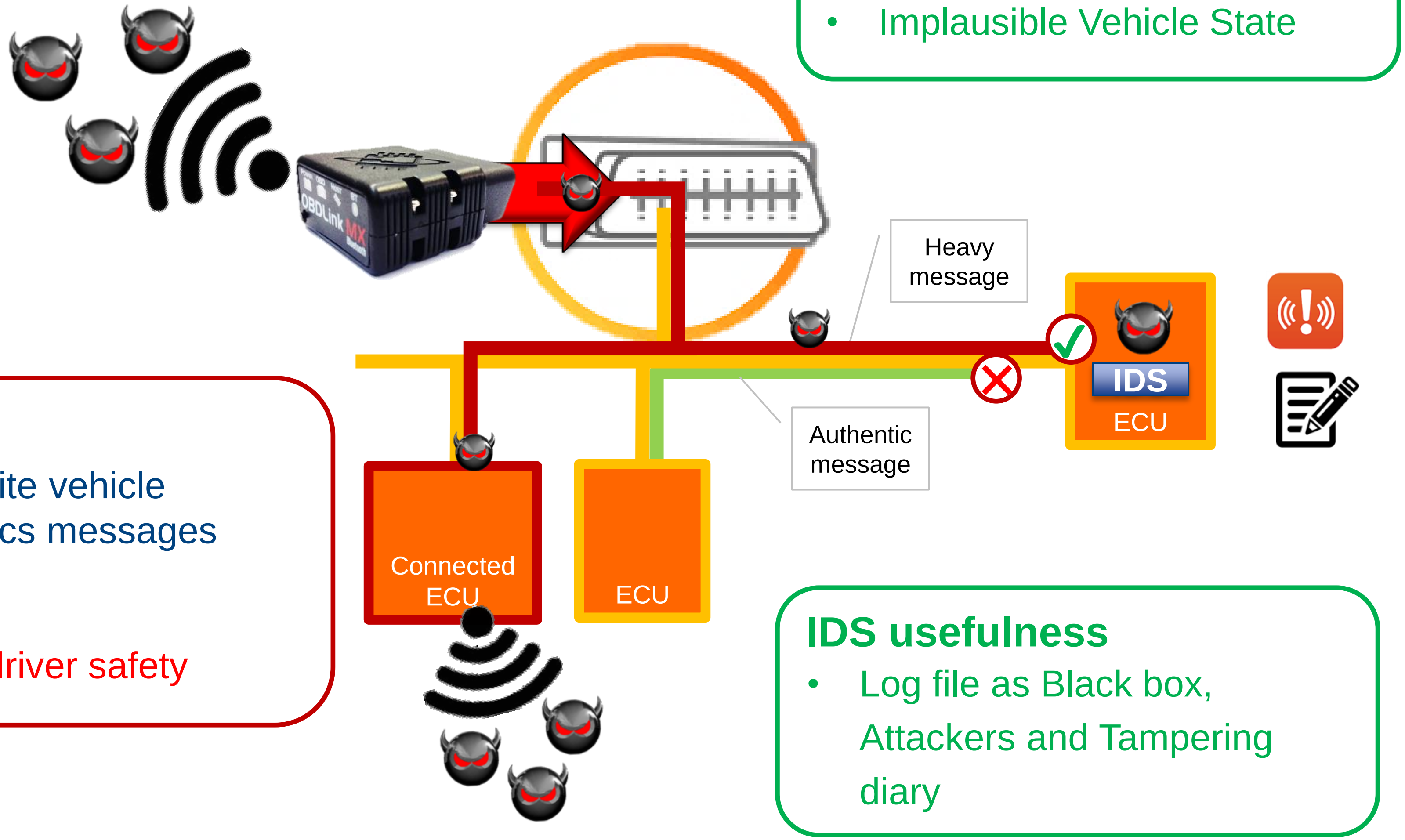
**Telematic Box**
Periodical log files upload

- *Black box*: helps to manage liability issues
- *Attackers diary*: helps to be update on the attacks
- *Tampering history:* helps to identify calibration tampering

- **Alarm to driver**
  - possibility to be advised in case of critical attacks

# Cyber Attacks I

## Cause an accident



**Identified anomalies**
- Invalid Rate
- Implausible Vehicle State

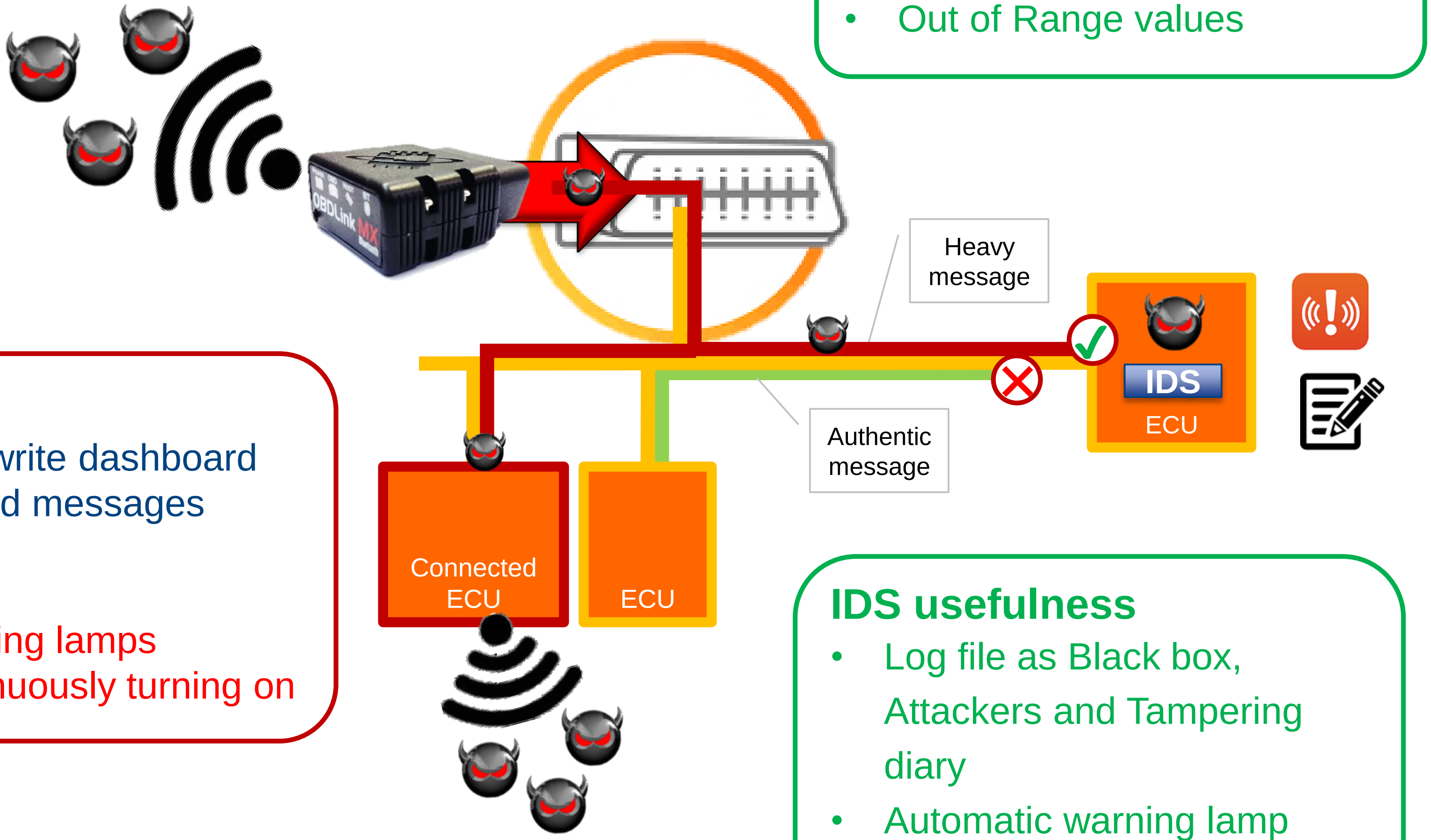
**Attack**
- Overwrite vehicle dynamics messages

**Effect**
- Affect driver safety

**IDS usefulness**
- Log file as Black box, Attackers and Tampering diary

# Cyber Attacks II

## Damage company’s image



**Identified anomalies**

- Invalid Rate
- Out of Range values

**Attack**

- Overwrite dashboard related messages

**Effect**

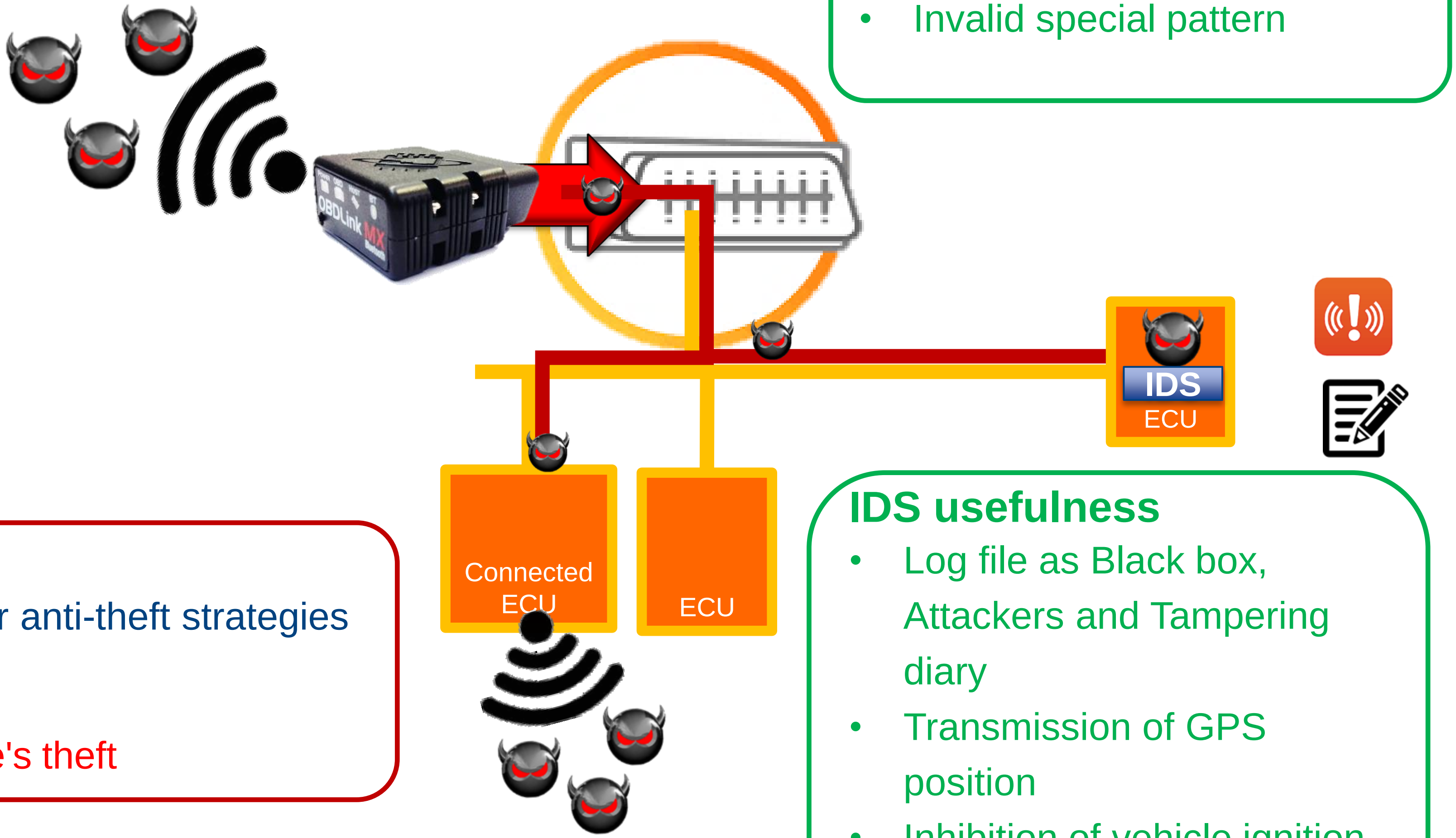
- Warning lamps continuously turning on

**IDS usefulness**

- Log file as Black box, Attackers and Tampering diary
- Automatic warning lamp reset

# Cyber Attacks III

## Cause a financial loss



**Identified anomalies**
- Invalid special pattern

**Attack**
- Tamper anti-theft strategies

**Effect**
- Vehicle's theft

**IDS usefulness**
- Log file as Black box, Attackers and Tampering diary
- Transmission of GPS position
- Inhibition of vehicle ignition on

# IDS: let's go a step further!

- **Coupling IDS with a recovery module**

**Intrusion Detection System**

Video surveillance system

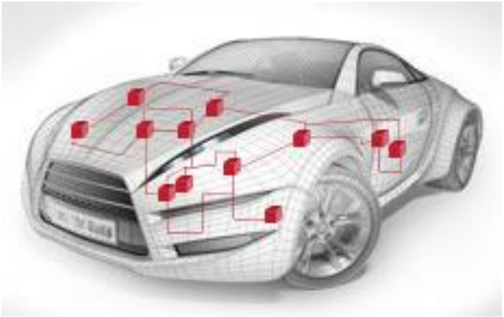
Monitoring the CAN frames transmitted on the bus

**Vehicle Recovery System**

Surveillance agent

Performing suitable actions, when an alert is raised by IDS

- **Modules deployment**



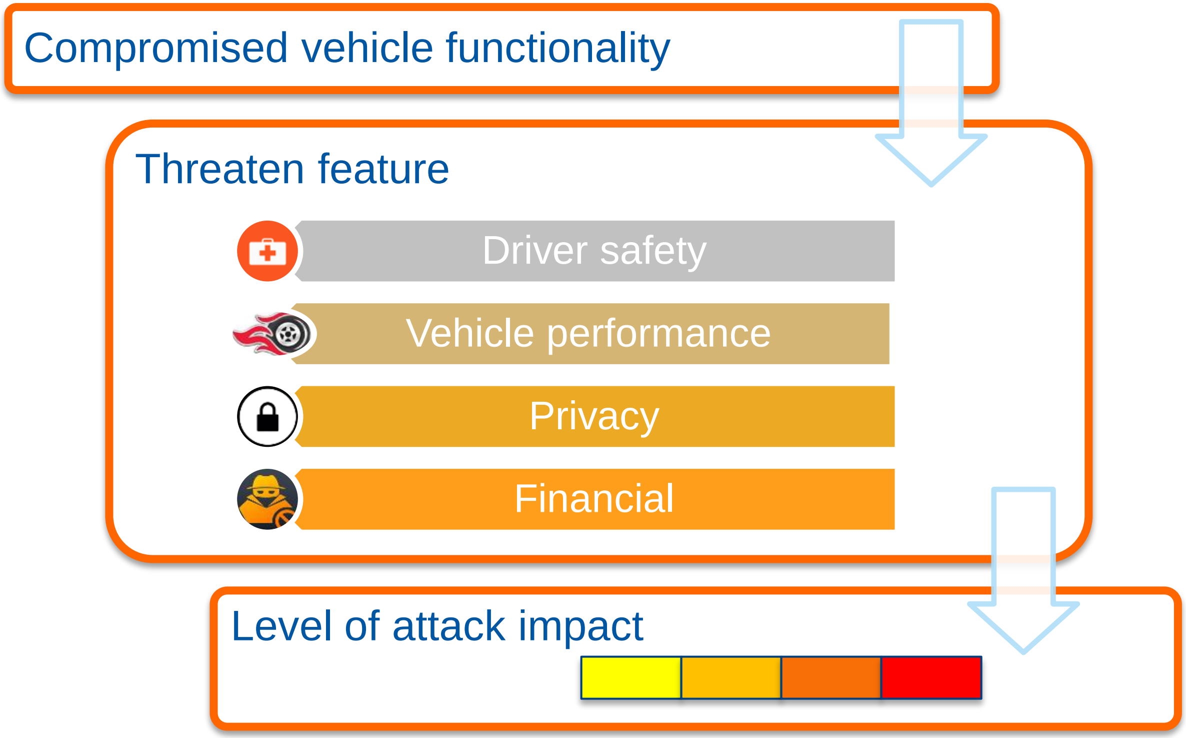
**Distributed IDS/VRS**

Each security critical node hosts the coupled modules

PATENT PENDING n. 102016000111869

# VRS: how could it work?

- **Recovery characterization**



Compromised vehicle functionality

Threaten feature

Driver safety

Vehicle performance

Privacy

Financial

Level of attack impact

🟨 🟧 🟧 🟥

- **Examples of recovery actions:**

▶ Reach the safety state

▶ Disable the compromised functionality

▶ Ignore the content of threaten CAN ID

▶ Inhibit diagnostic service

# Conclusions

- Vehicles network vulnerability is increasing due to the enhancement of connectivity

- Cyber attacks are a risk also for low connected vehicles

- Intrusion Detection System allows
  - monitoring of CAN traffic
  - recording of identified anomalies

- Starting from IDS anomalies, Vehicle Recovery System is able to perform suitable strategies to reduce the cyber risk

Anastasia Cornelio
anastasia.cornelio@magnetimarelli.com

Elisa Bragaglia
elisa.bragaglia@magnetimarelli.com

**Magneti Marelli – Technology Innovation SSEC**
Via del Timavo 33 - 40134 Bologna, Italy
www.magnetimarelli.com