sentryo

Cyber Security for the **Industrial Internet**

L'importance de la détection des cyberattaques dans les véhicules connectés et autonomes

Sentryo HQ | 66 Bd Niels Bohr CS 52132 69603 Lyon-Villeurbanne - France
+33 970 469 694 | contact@sentryo.net | www.sentryo.net

Laurent Hausermann - Founder

laurent.hausermann@sentryo.net
+33 (0) 617 108 433

Nicolas Justin

nicolas.justin@sentryo.net
+33 (0) 608 248 978

Company Overview

- **Incorporated:** June 2014
- **Headquarters:** Lyon - France
- **Venture capital** backed by UK/FR funds
- Target **Industrial corporations:** Energy, Process Industries, Manufacturing, Transportation
- Offices: **France/Germany/USA**
- Partners: **USA, LATAM, South Asia, Middle East**

Awards

BMW TechDate **Winner** - June 2016

CISCO Acceleration **Prize** - June 2016

Lauréat Concours Mondial de l'Innovation CMI - June 2016

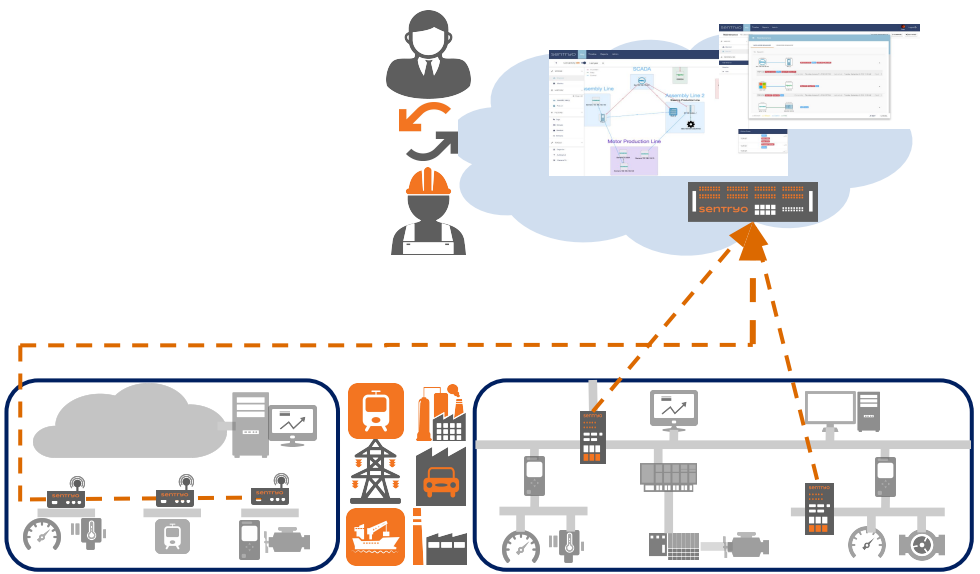
Winner Innovation Prize Monaco Cybersecurity Show October 2015

IIOT Cybersecurity startup of the year McRock Capital Symposium - May 2017

Sentryo Automotive Detection Project

Extend our existing technology stack for Industrial Networks (ie Production, ICS) to embedded IoT, M2M & Automotive networks

INNOVATION 2030
CONCOURS MONDIAL D'INNOVATION



#Monitoring

#AnomalyDetection

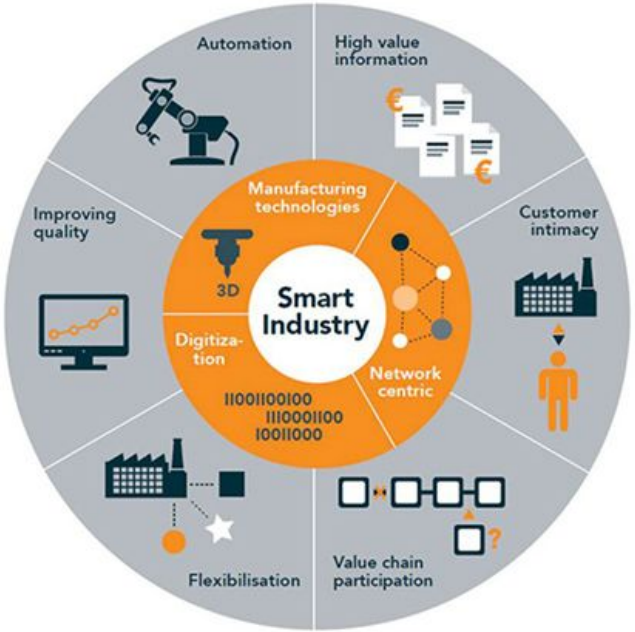
#MachineLearning

#CANBus

#AutomotiveEthernet

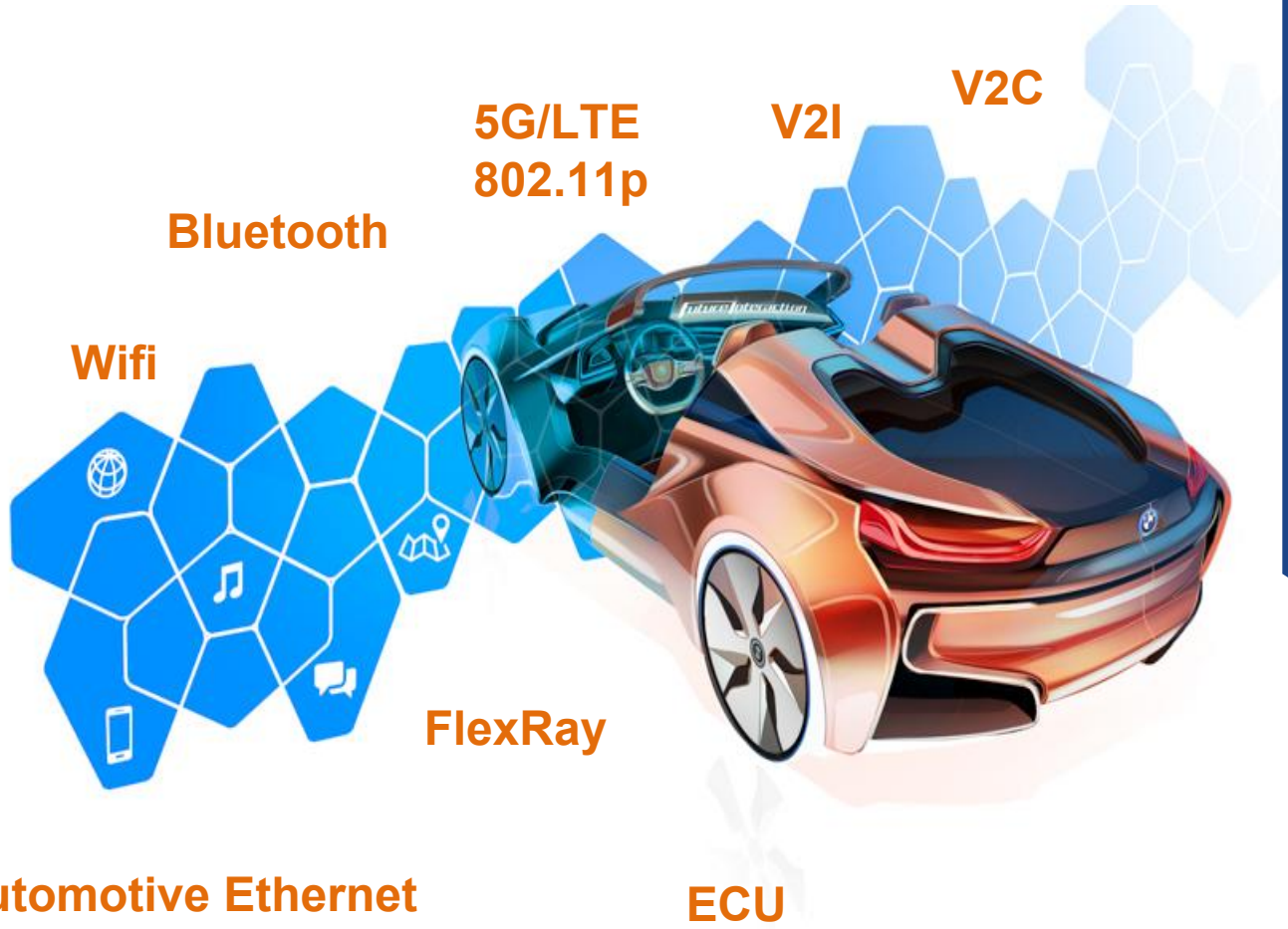
New challenges for industrial corporations

IT & OT & IIoT - A fast changing converging environment



IoT & Fog Computing - A new digital paradigm for automotive ecosystem

Business Challenges

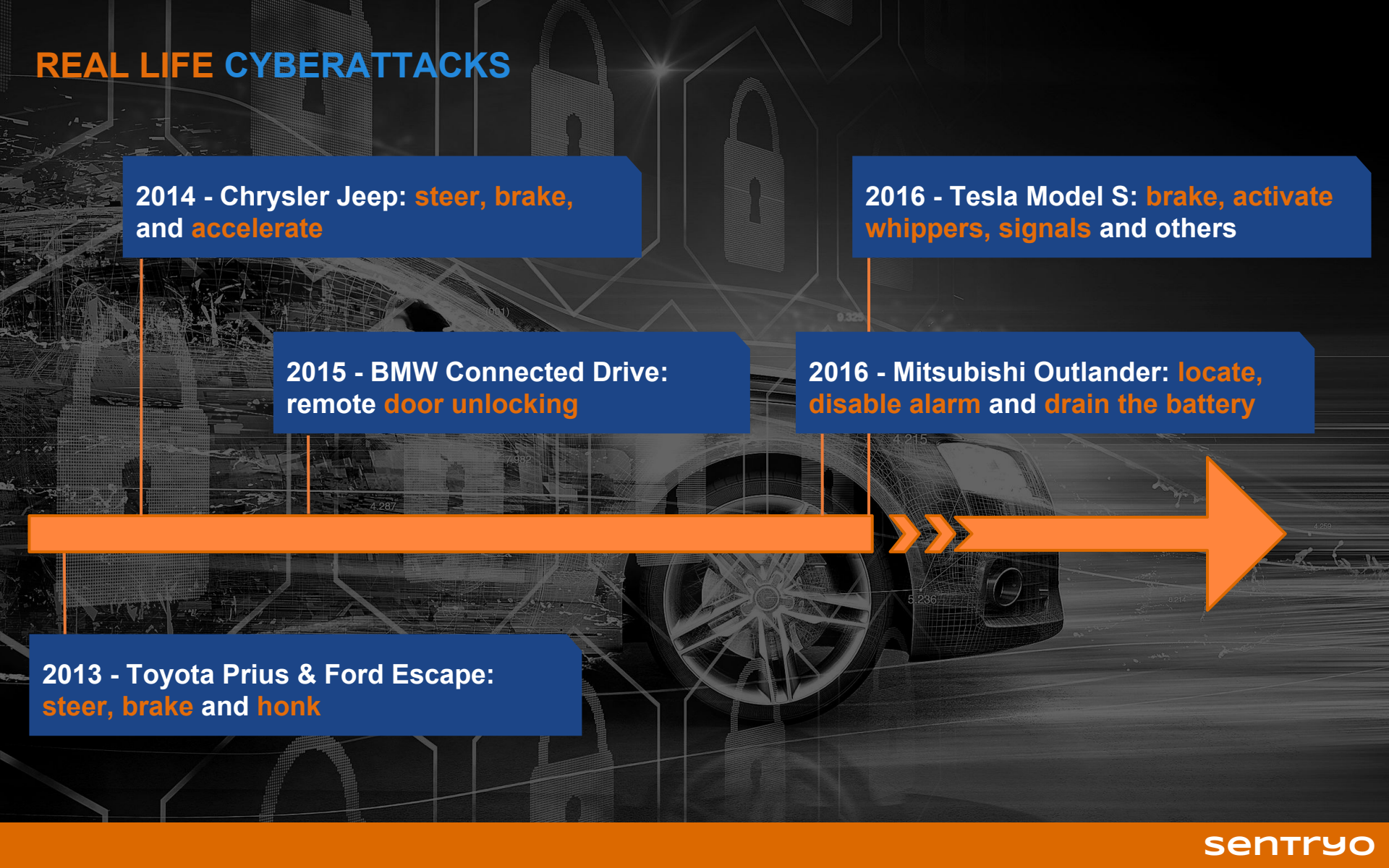


New Services
Driving assistance, Internet, Entertainment…

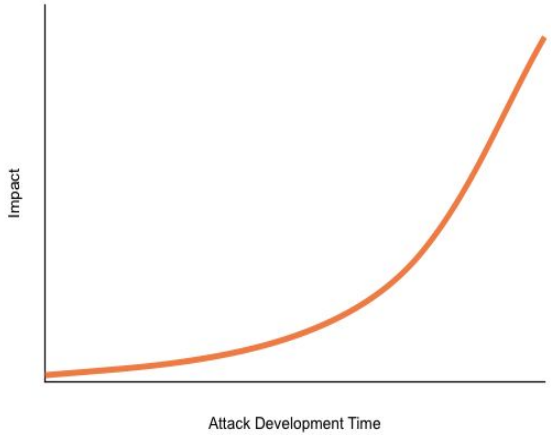
New Businesses
Energy savings, Car sharing, Automated parking...

Customer Trust ?

REAL LIFE CYBERATTACKS

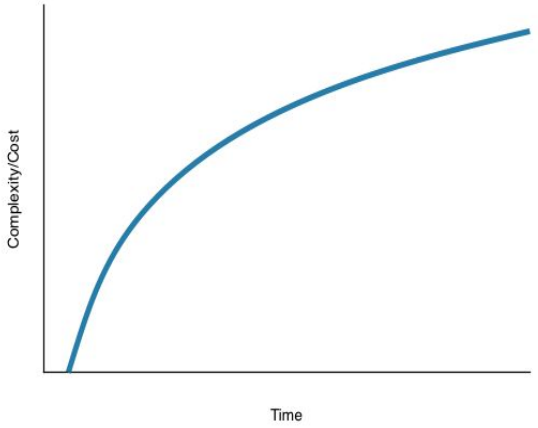


Hackers vs Automakers



Hackers

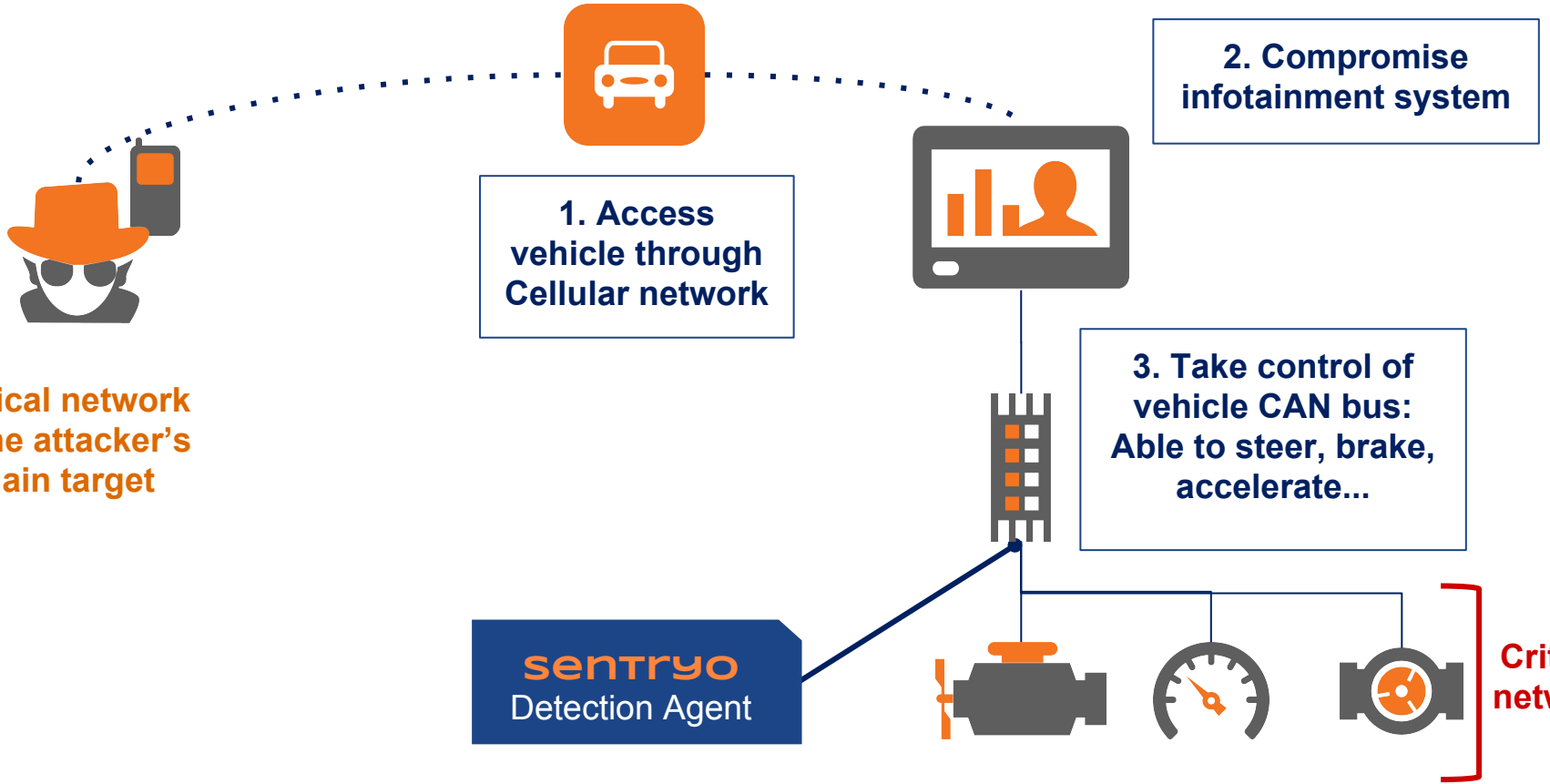
- Lot of time available
- Undetectable vulnerability research
- Large attack surface
- High damage potential
- Ease of replication without large resources



Automakers

- Overall safety is a bigger subject
- Long development cycle
- Need full control over source code
- Low resources for cybersecurity
- CAPEX >> OPEX

Attackers Steps



Attacks vs Anomalies

Attacks

- Discover vehicle components: scanning
- Disturb vehicle: Denial of Service, ransomware...
- Search security holes and potential bugs: fuzzing
- Get access to firmware, modify critical parameters (ABS…)

Anomalies

- Industrial or M2M protocol are really basics, legit orders are similar to attackers orders
- Can be subtle to slowly damage critical components
- Can be a system anomaly or due to a cyberattack

On critical networks Attacks and Anomalies must be detected

Detection Approach

Attacker's steps

1. Gain access to Infotainment
2. Scan all vehicles ECUs
3. Silence collision prevention
4. Send false values to Autocruise

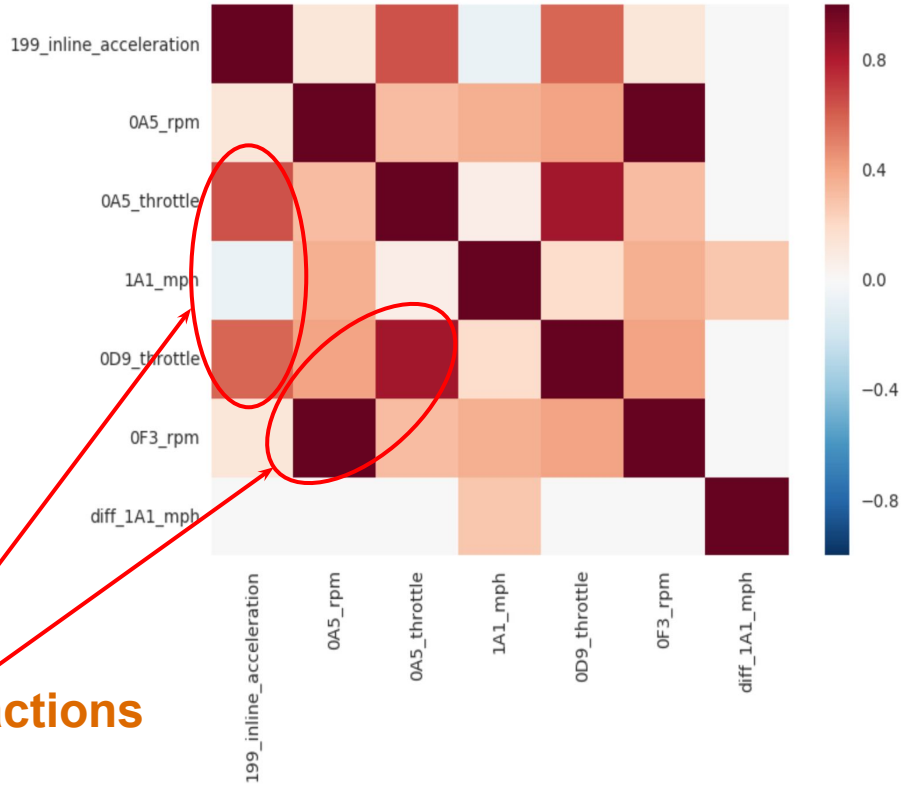
Detection Methods

Attack:
- Scanning
- Denial of Service

Anomaly:
- Deviation of vehicle's Speed despite the distance with a front obstacle

Advanced anomaly detection

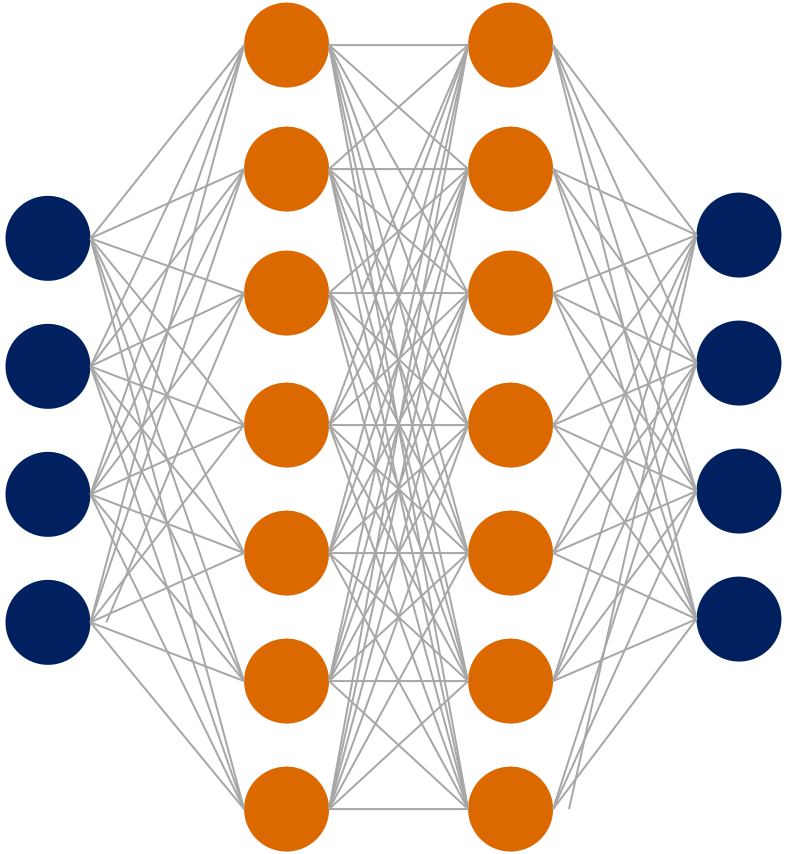
- Lot of in-car sensors values can be correlated
- One sensor value can be reconstructed using a set of other sensors values
- Each sensors can be reconstructed using others



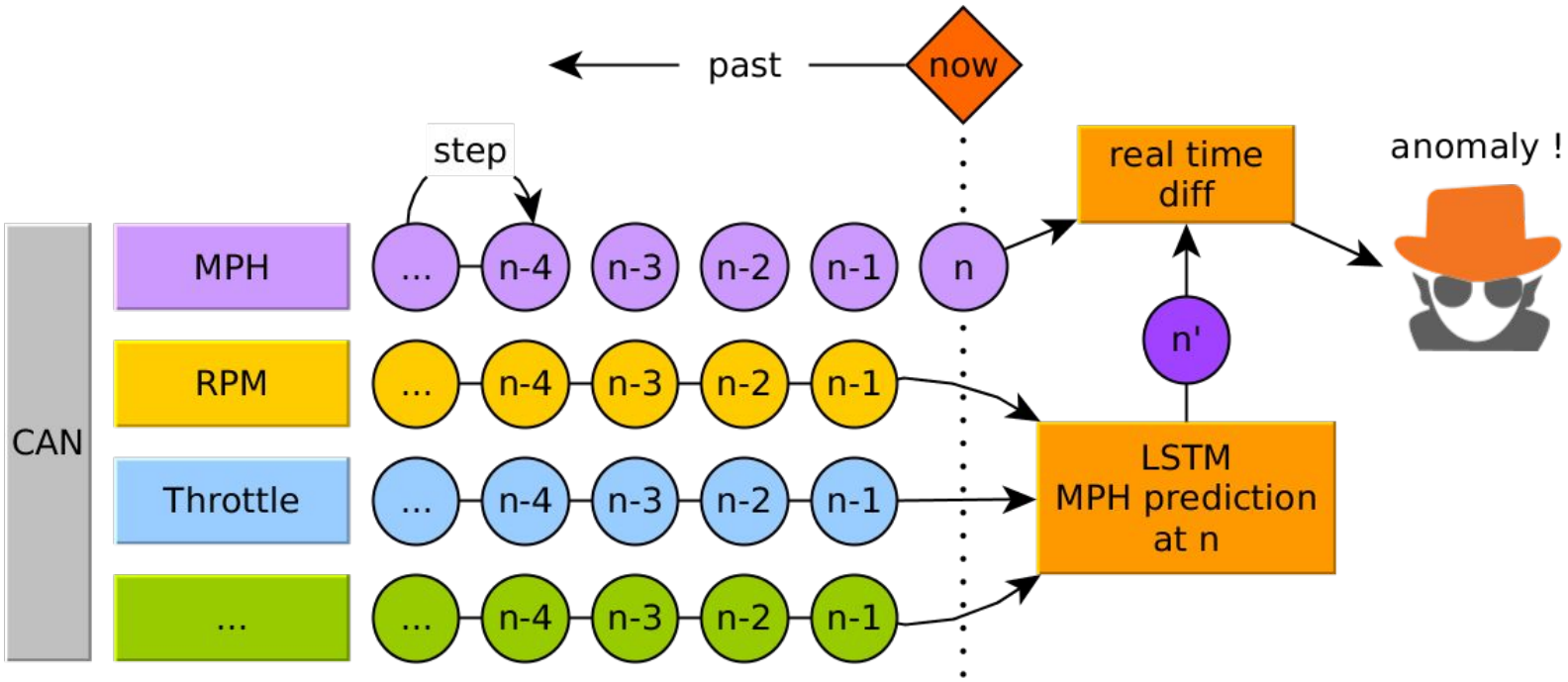
Strong interactions

Neural Networks

- Neural Networks are perfectly adapted to find and learn correlations in complex systems
- Neural Networks can make good prediction
- High prediction error means anomaly

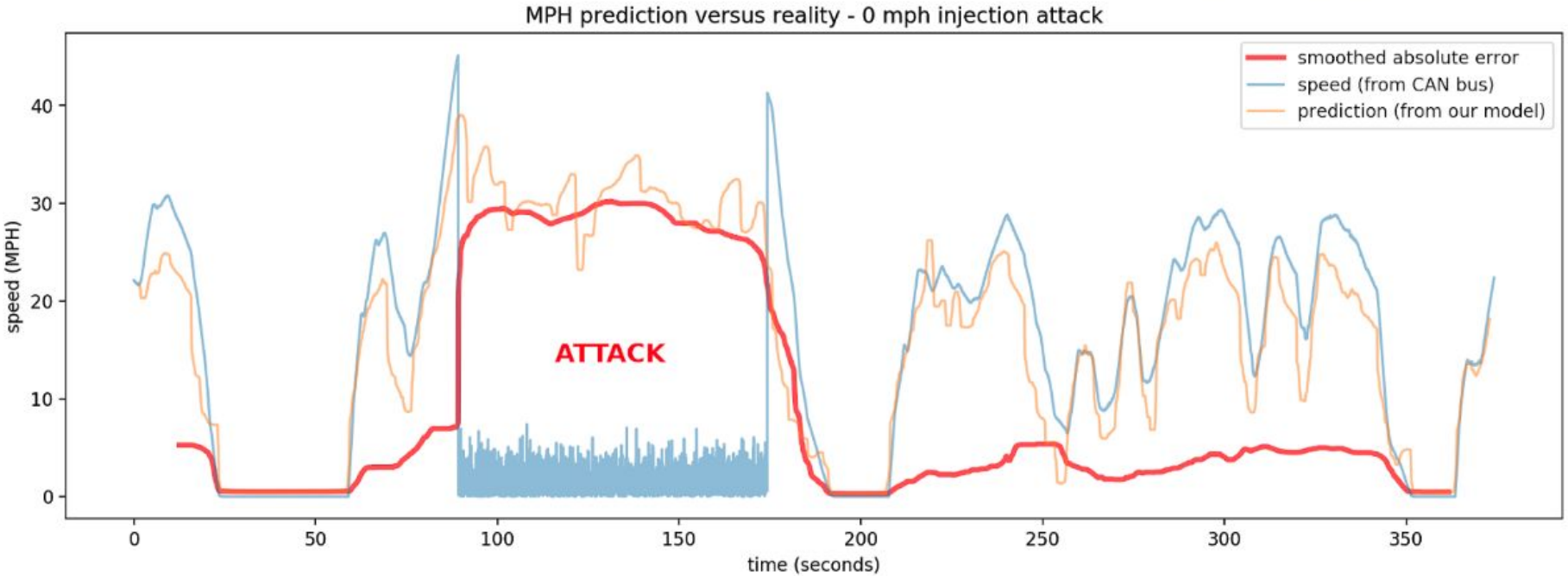


MPH anomaly detection



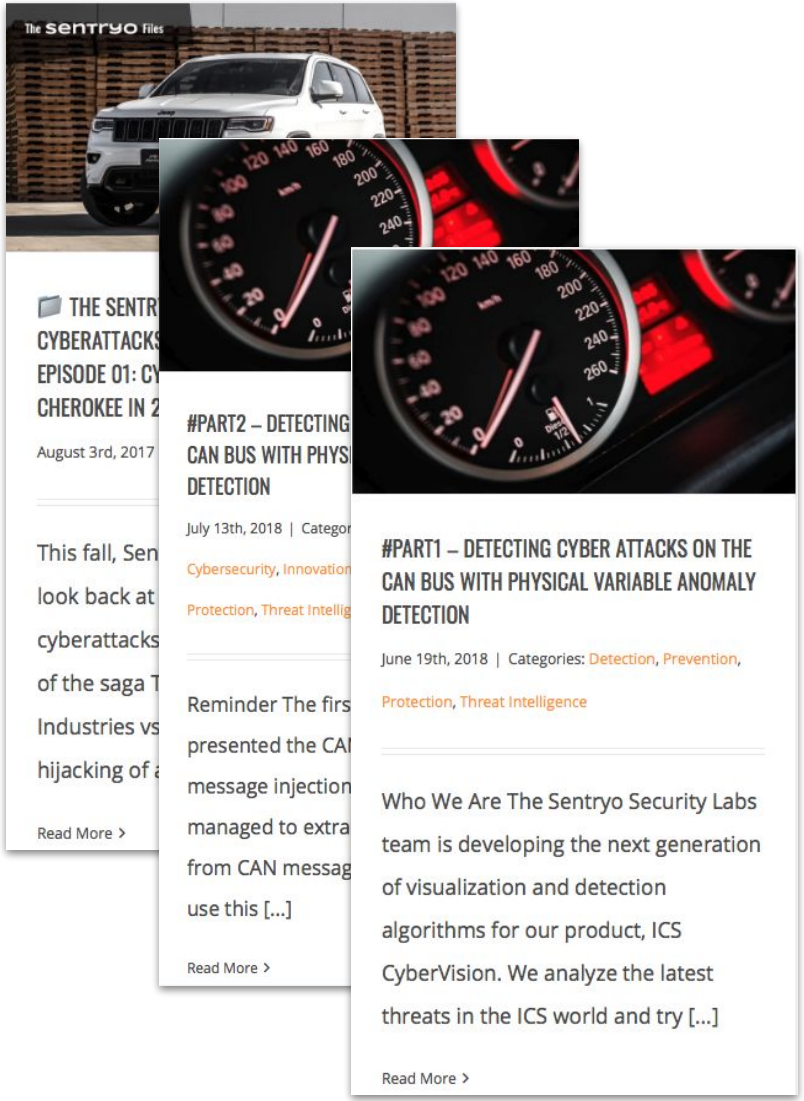
MPH anomaly detection

- In case of attacks the prediction error ratio will be high
- Attacker injected a 0 MPH speed value on the bus to trick the Park Assist for example



More information on Sentryo's blog:

https://www.sentryo.net/blog/



Gartner
Cool Vendor
2018