# Cyber Security support to the HumanDrive Project

13th Dec 2018

SBD Automotive Ltd

Luigi Bisbiglia Business Development Manager

HUMAN DRIVE

Using machine learning to develop

**natural, human like vehicle control**

# Using machine learning to develop natural, human like vehicle control

The BIG Ambition

Grand Drive

Autonomous Drive

- ‘Grand Drive’ will be an end-to-end journey of around 200 miles including Motorway, A-Road and Country Road driving
- Using Machine Learning and AI to provide human-like control
- Research into human driving behaviour using physical vehicles and simulator
- Transport Systems Catapult and Horiba MIRA responsible for the Safety Work Package
- Cyber Security covered by a separate Work Package

**2017**

July 2017
Project Start

**2018**

Autumn 2018
Static Environment Trials

**2019**

Summer 2019
Dynamic Trials

Winter 2019
Grand Drive

Dec 2019
Project Complete

HUMAN DRIVE

NISSAN HITACHI Inspire the Next Cranfield University MIRA aimsun. UNIVERSITY OF LEEDS ATKINS highways england CATAPULT Transport Systems SBD

HumanDrive.co.uk @HumanDriveCav HumanDriveCav

We work with Innovate UK

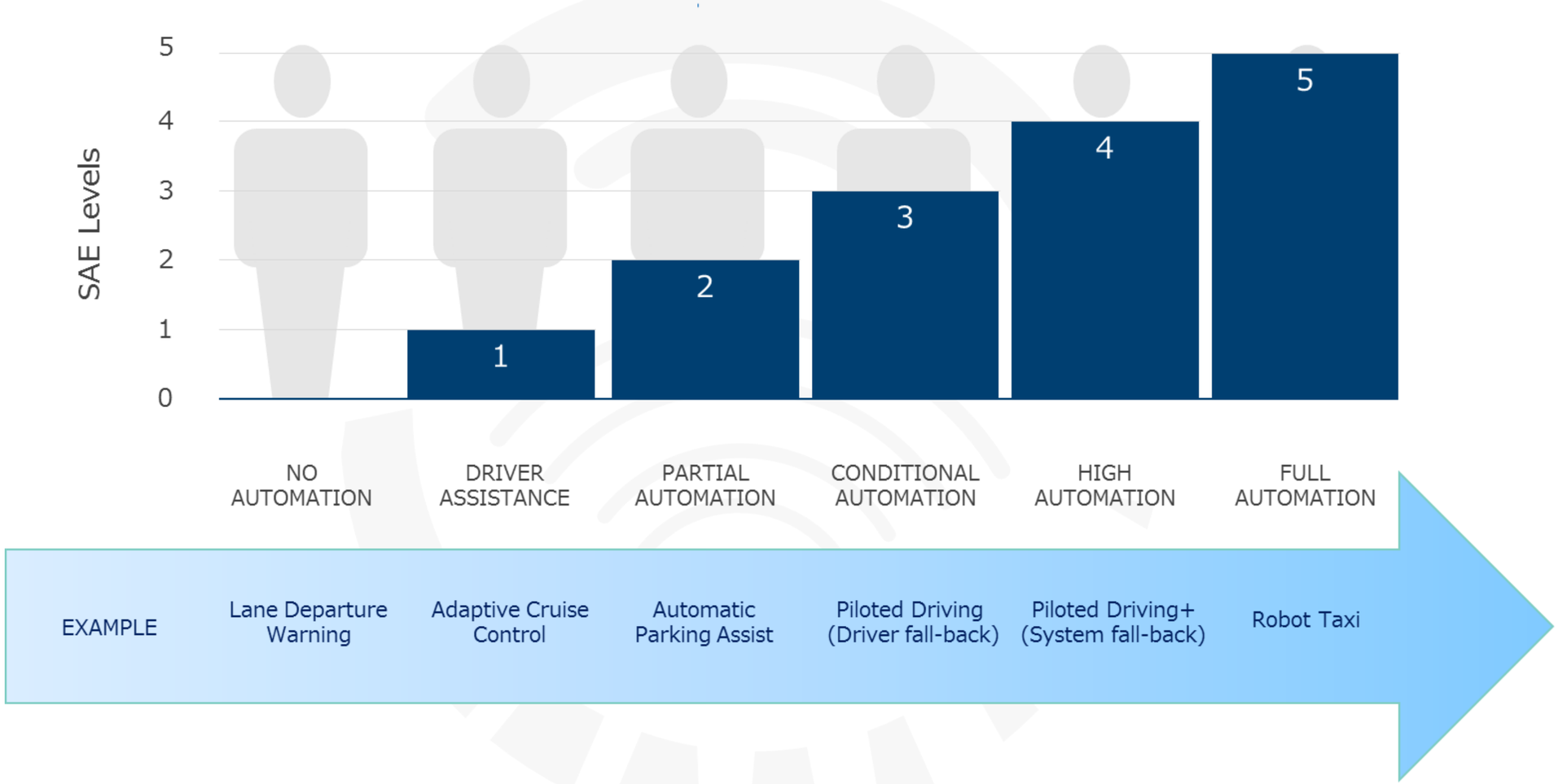
# SBD’s Cyber Support Package


- Analysis of public hacks
- New product and technology tracking
- New standards and guidelines
- Competitor activity
- Knowledge sharing

- Threat modelling for security requirements and design reviews
- Penetration testing
- Risk assessment (analysis of results, remediation and risk rating)

- Objective setting
- Design process improvement
- Cyber roadmap
- Incident response planning
- Training
- Supplier evaluation

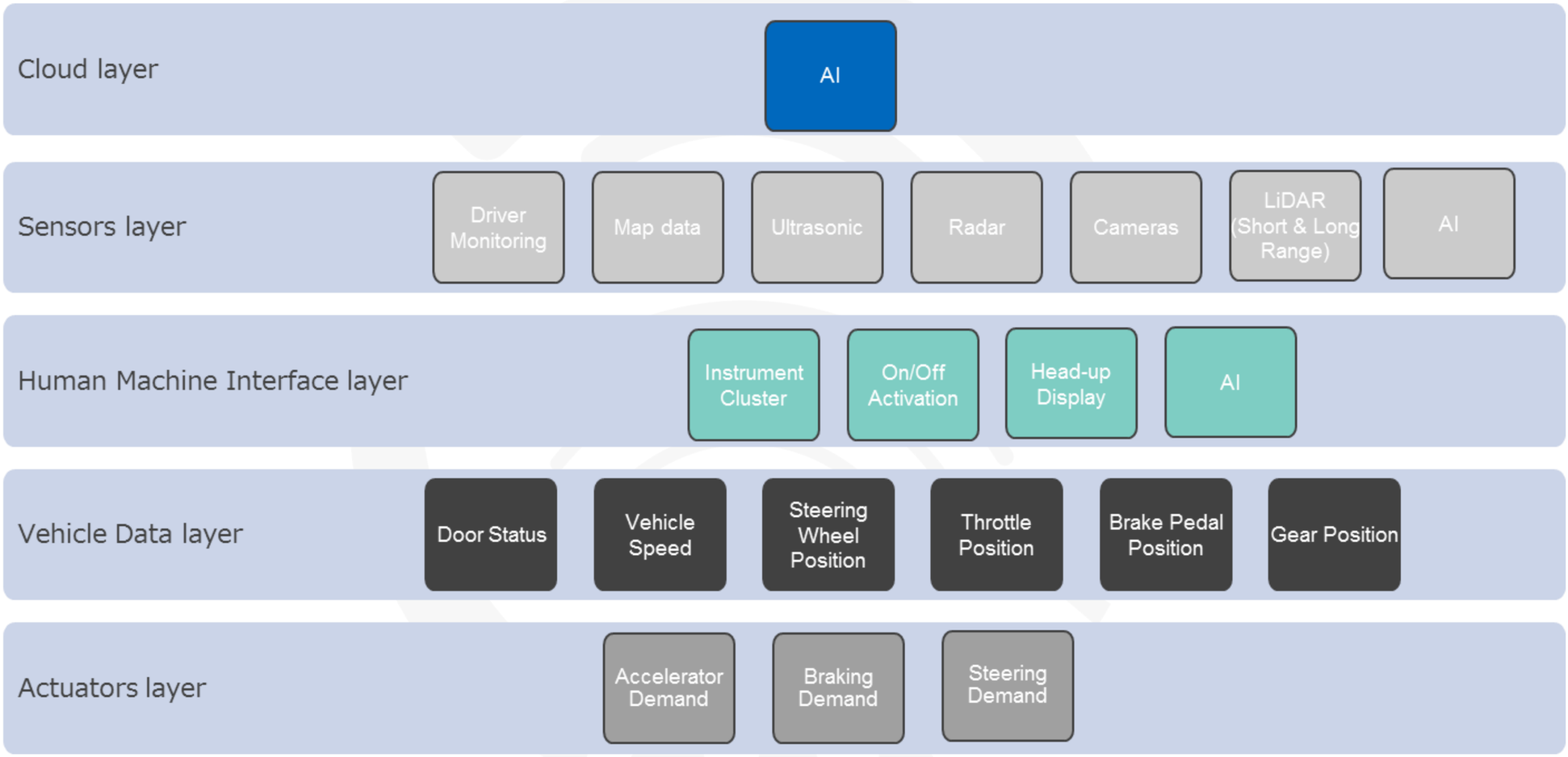
# SAE Definitions



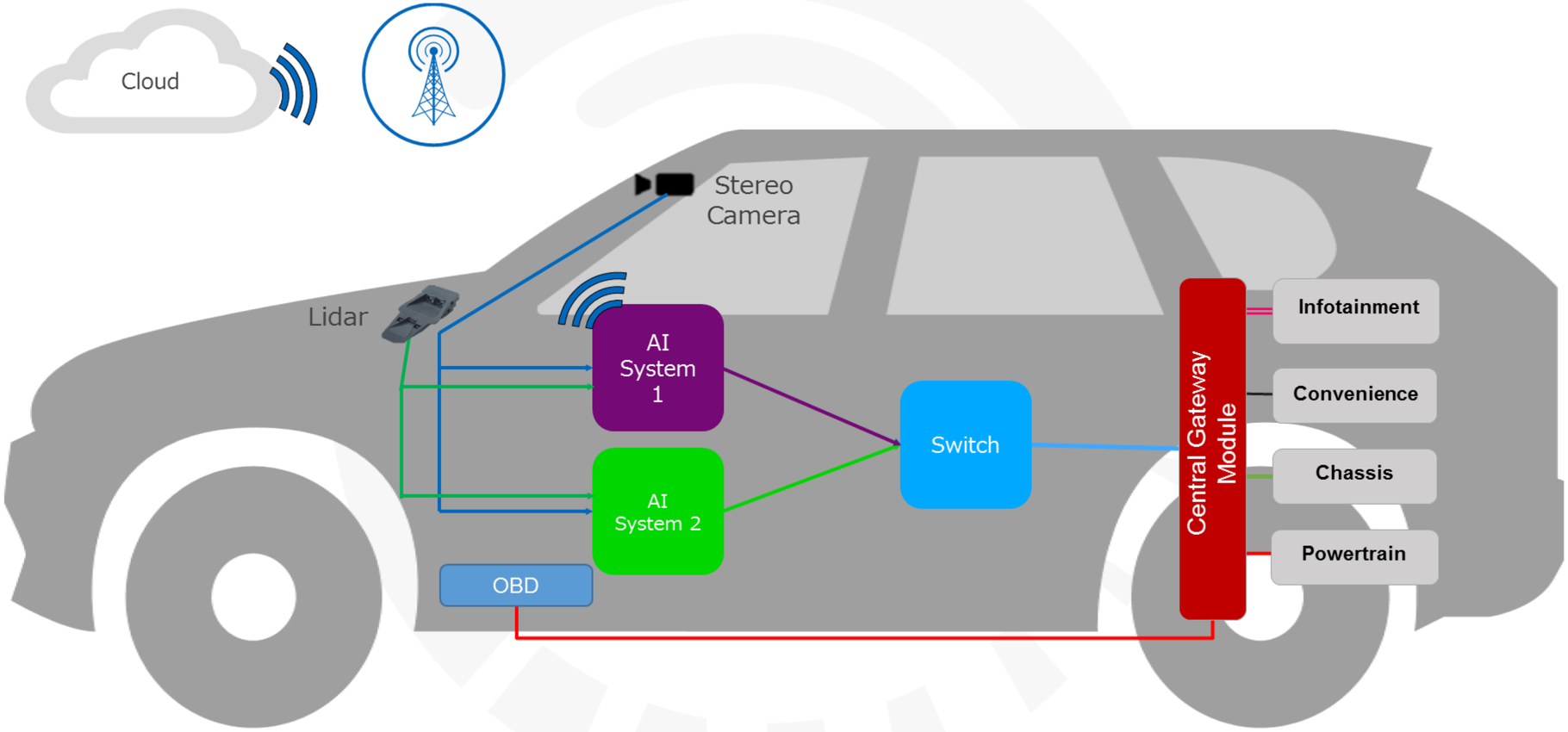
# Implementation Trends

| SAE Levels | Key in-car architecture characteristics |
|---|---|
| **Level 0**<br>“Legacy architecture” | • Piece meal implementation<br>• Very few ADAS available, developed as a stand alone solution<br>• No sensor fusion (**sensor hardwired to ECU, not networked**) and no actuators involved<br>• **Mainly CAN technology** |
| **Level 1**<br>“Carry-over architecture” | • Piece meal implementation<br>• A few stand-alone ADAS<br>• When there is actuation (e.g. braking), **the ADAS ECU is usually on the same network as the actuator**<br>• **Mainly CAN technology** |
| **Level 2**<br>“Primitive ADAS architecture” | • **Dedicated ADAS network**<br>• Primitive / localised sensor fusion taking place (front sensing with rear facing). Some sensors are networked<br>• **FlexRay technology introduced**<br>• **Ethernet used for 360 all round view**<br>• **Some features communicate with key fob / smartphone** |
| **Level 3**<br>“Semi autonomous architecture” | • **Dedicated ADAS domain** to support sensor fusion on a much larger scale<br>• Sensor fusion partitioned in domains<br>• GPS / map data becomes a sensor that needs **regular update**<br>• **Communication with key fob / smartphone**<br>• **FlexRay and Ethernet standard** |
| **Level 4**<br>“Full autonomous architecture” | • Dedicated ADAS domain to support full sensor fusion (Forward, Rear, All Around)<br>• GPS / map data need near “real-time” update & high definition<br>• **Communicate with key fob / smartphone**<br>• **OTA download and connected services (including Artificial intelligence)**<br>• FlexRay and Ethernet standard |
| **Level 5**<br>“Driverless architecture” | • Same as for level 4 but with more sensors to accommodate all types of road, weather and lighting environment. |

# Layer 3 and above layers architecture



# Representative Electrical Architecture



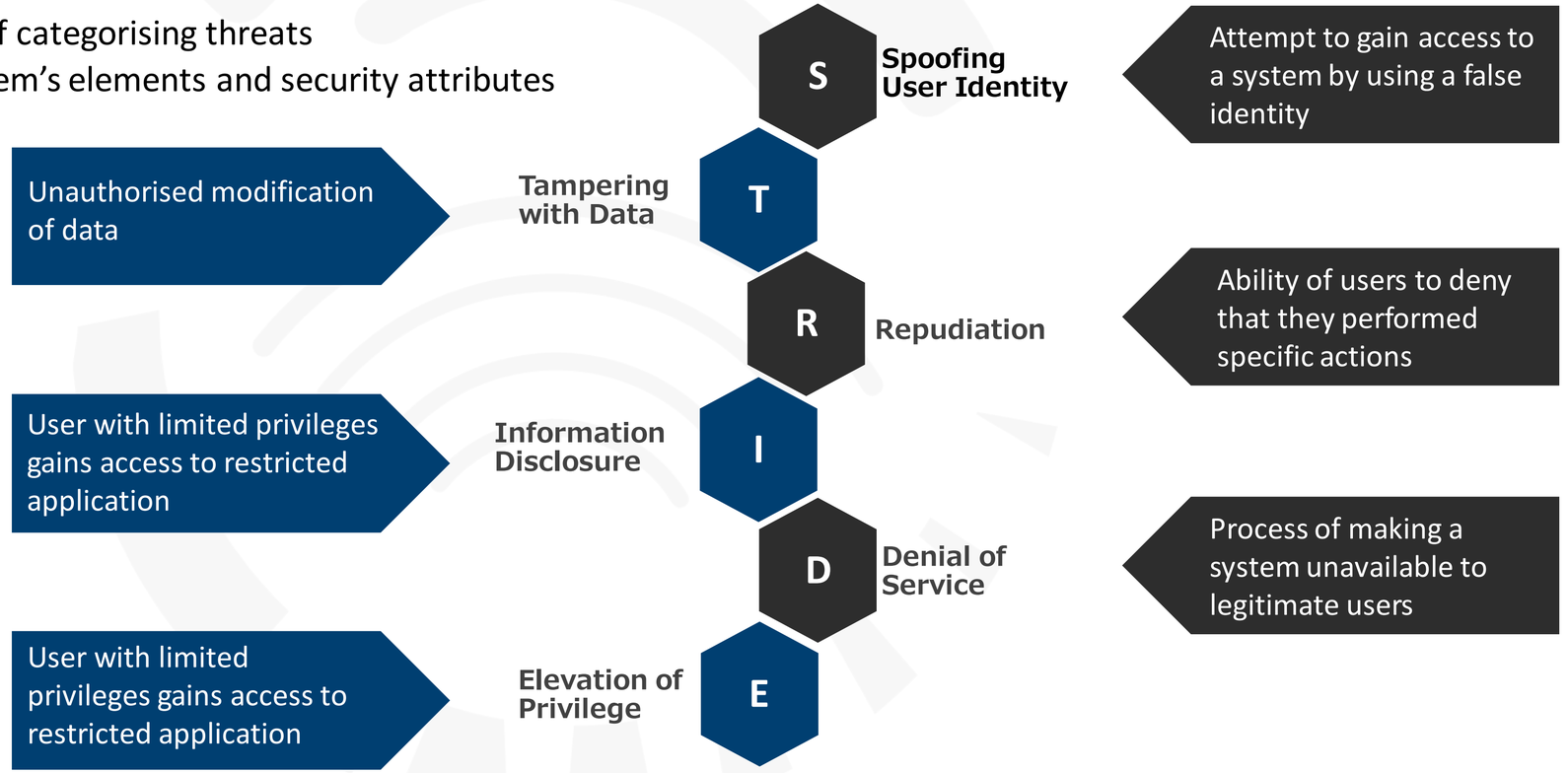

Using machine learning to develop
**natural, human like vehicle control**

HUMAN DRIVE

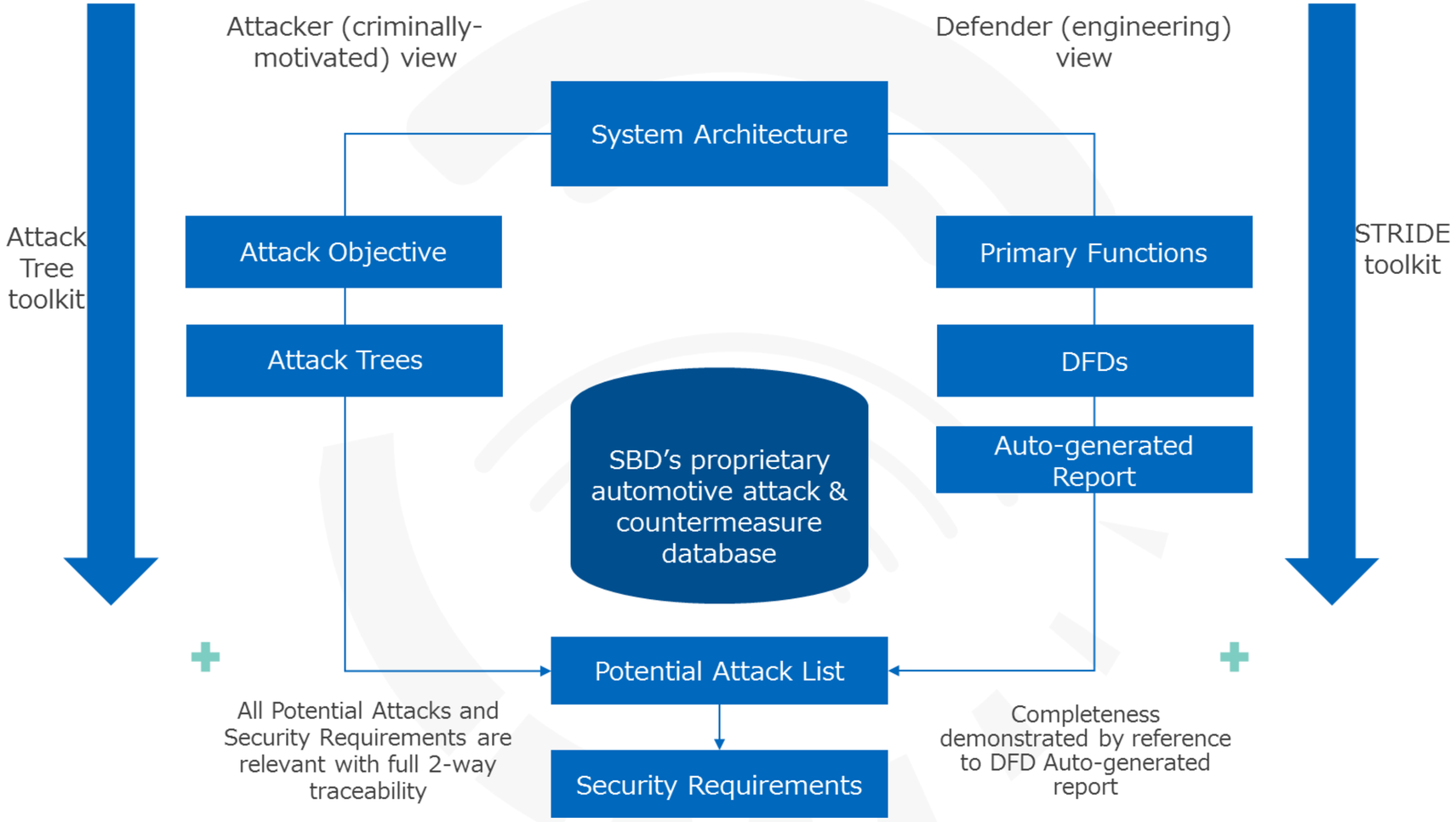
# STRIDE

STRIDE (**S**poofing, **T**ampering, **R**epudiation, **I**nformation **D**isclosure, Denial of Service and **E**levation of Privilege) is a threat modelling approach developed by Microsoft and it is currently considered the most applicable method for the automotive industry because it:

- Is a threat centric approach
- Provides a structured approach of categorising threats
- Enables direct mapping with system's elements and security attributes



# Threat Modelling

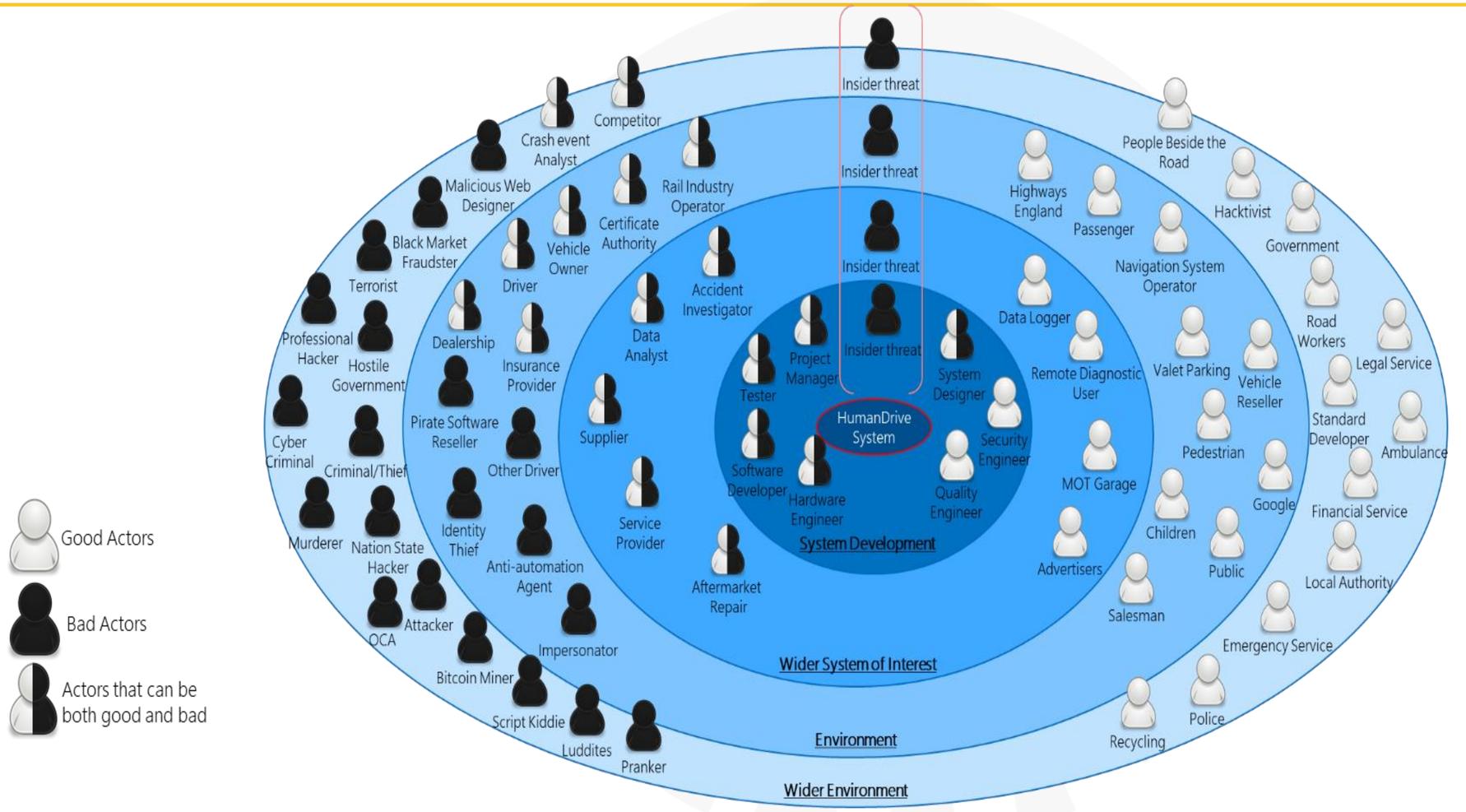


# Reference: Who are the Hackers ?

- Depending on hackers/hacker groups, targets can be different. Therefore attacking techniques and equipment are also different.

| | | |
|---|---|---|
|  | Hactivists | Make Political Statements |
|  | Cyber Criminal | Financial gain, Cyber Warfare |
|  | Disgruntled ex-employees | Revenge |
|  | State Hackers | Espionage |
|  | Script Kiddies | Fun and Fame, Avoid paying |
|  | Spy Hackers | Corporate Espionage |

# Defining the Actors Environment

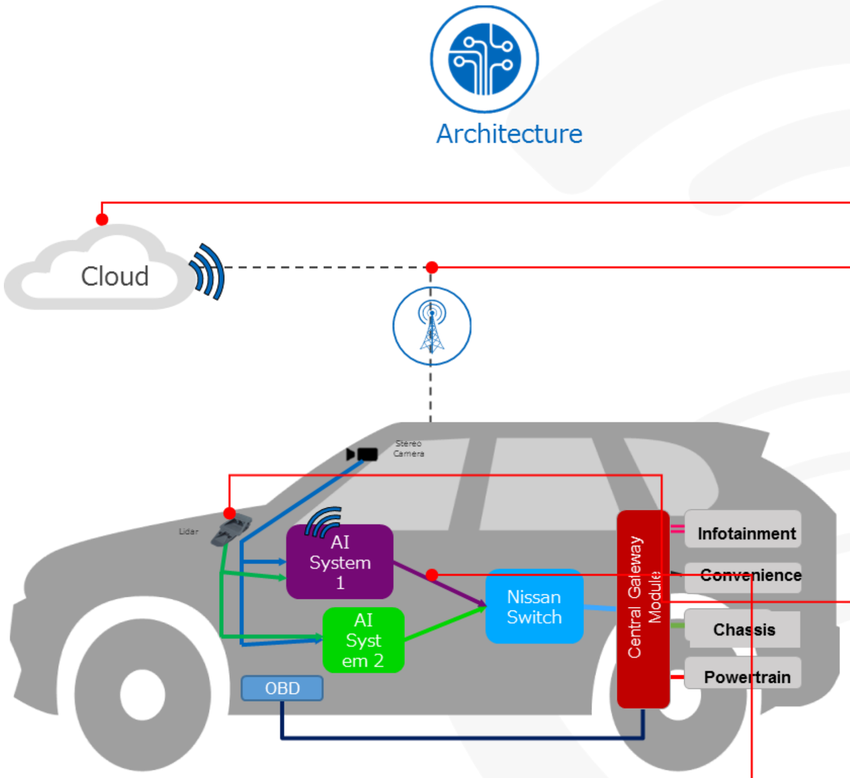


# Representative Abuse Stories

- User stories is a method for capturing high-level system functional requirements. The user stories are generated by the system stakeholders.
- User stories captured for **malicious** Actors can help in identifying potential **system misuse or exploitation**, at a high level.
- User stories written for intended Actors can help in identifying the functions that need protecting and the required interactions between the intended Actors.

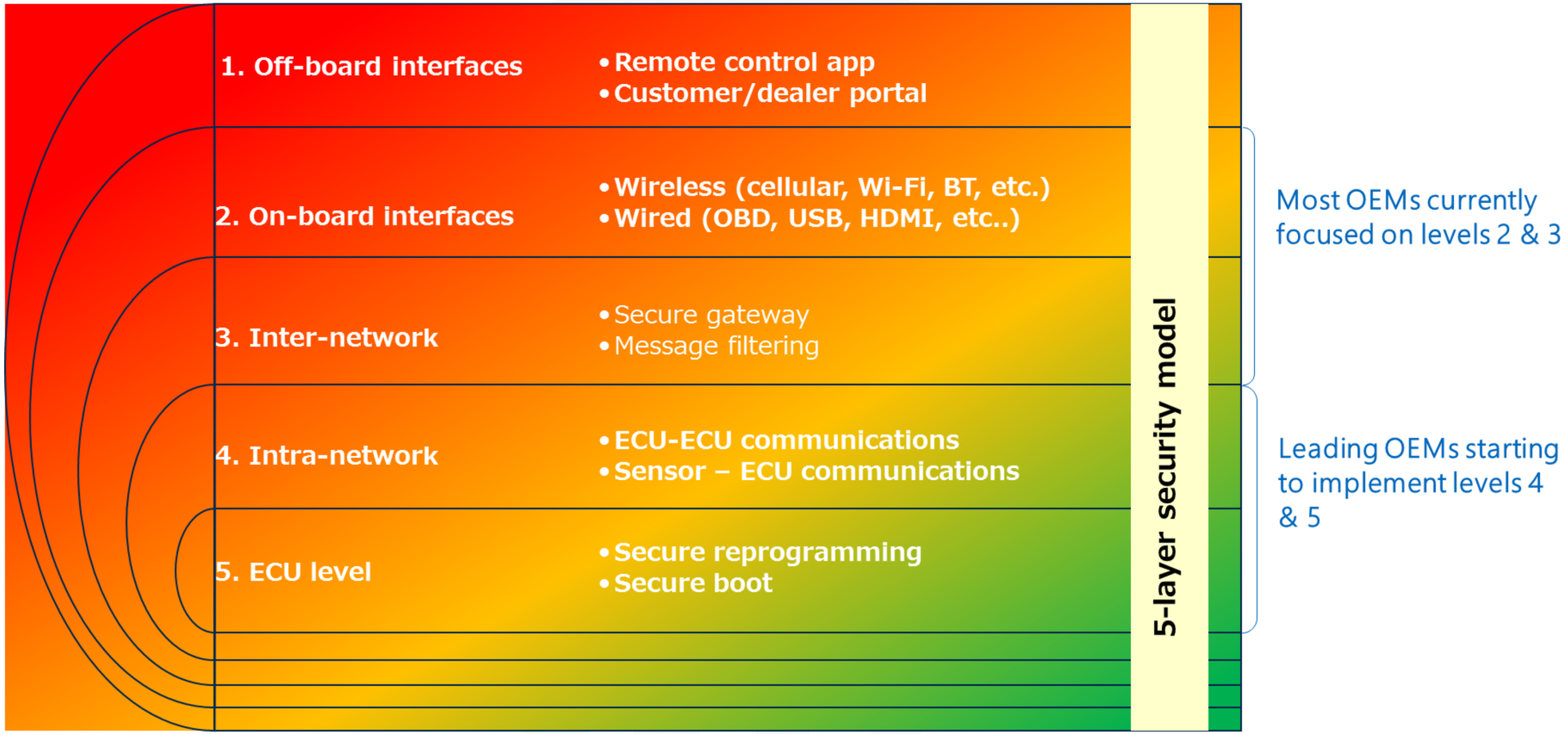
| Case # | Actor | I Want | So That |
|---|---|---|---|
| 1 | Bitcoin Miner | Use ability of ECUs | Get more bitcoin |
| 2 | Academic Researcher/Cyber Criminal | Spoof the system | Get private information from vehicle |
| 3 | Service Provider | Patch the vehicle but ignore some of them | Have this customer back and get more money |
| 4 | Vehicle Owner | Block the entrance parking | Annoy my neighbours |
| 5 | Vehicle Owner | Cheat after cars into giving ways | He can drive faster |
| 6 | Professional Hacker | Hack into the car | Ransom it to their owners |
| 7 | Competitor | Cause delays(jam) in some roads | Gain advantage/value |
| 8 | Criminal | Follow another vehicle | Do criminal activities |
| 9 | Criminal | Other CAV crash into my own | Get money |
| 10 | Criminal | Use Autonomous Car | Transport illicit goods |
| 11 | Terrorist | Use Autonomous Car | Damage traffic |
| 12 | Professional Hacker | Spoof signs | Change vehicle behaviour |
| 13 | OCA (Organise Crime Agent) | Data mining - sell products on web | Can get profit |
| 14 | OEM | Gather data to sell | Get money |
| 15 | Competitor | Develop new exciting products | Seize the market |
| 16 | Pranker | Direct traffic | Make giggles |
| 17 | OEM | Highlight deficiencies in system | Gan greater market sharing |
| 18 | Attacker/Terrorist | Remotely control cars | Commit a terrorist attack |
| 19 | Professional Hacker | Control the vehicle | Do the DDoS attack to others |

# Defence In Depth




| Attack Methods | Countermeasures |
|---|---|
| AI Model Tampering | ▪ Input validation and sanitization<br>▪ Access control with authorisation and authentication |
| AI Model Tampering during OTA | ▪ Have a secure point to point communication channel which prevents data from being manipulated while it is in transit. |
| Spoofing the LiDAR to trick the AI Based | ▪ Cross reference data from multiple sensors to establish the validity of the data/observations |
| Gain access to the Ethernet connection and replay misleading data | ▪ Disable all the unused services on the switch (i.e. developer ports)<br>▪ Configure Port Security and specify what action to be taken when a violation occurs (i.e shutdown)<br>▪ Add port base authentication<br>▪ Apply anti-replay protection techniques |

# Defence in Depth



# HumanDrive Consortium











http://humandrive.co.uk

Richard.Hillman@ts.catapult.org.uk

**Using machine learning to develop natural, human like vehicle control**

HUMAN DRIVE