Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle

Jianhao Liu 360 ADLAB SKY-GO Team

Chen Yan Zhejiang University

Wenyuan Xu Zhejiang University & University of South Carolina

Who Am I

Paddy Liu

Director of Qihoo360 ADLAB

SKY-GO Team Vehicle Cyber Security

Jianhao Liu is a senior security consultant at Qihoo 360 who focuses on the security of Internet of Things and Internet of Vehicles. He has reported a security vulnerability of Tesla Model S, led a security research on the remote control of a BYD car, and participated in the drafting of security standards among the automobile society. Being a security expert employed by various information security organizations and companies, he is well experienced in security service, security evaluation, and penetration test.

Who Am I

Chen Yan

Ph.D. Student

Ubiquitous System Security Laboratory (USSLAB)

Zhejiang University, China

His research focuses on the security and privacy of wireless communication and embedded systems, including automobile, analog sensors, and IoT devices.

Who Am I

Wenyuan Xu

Professor

Zhejiang University, China

University of South Carolina, United States

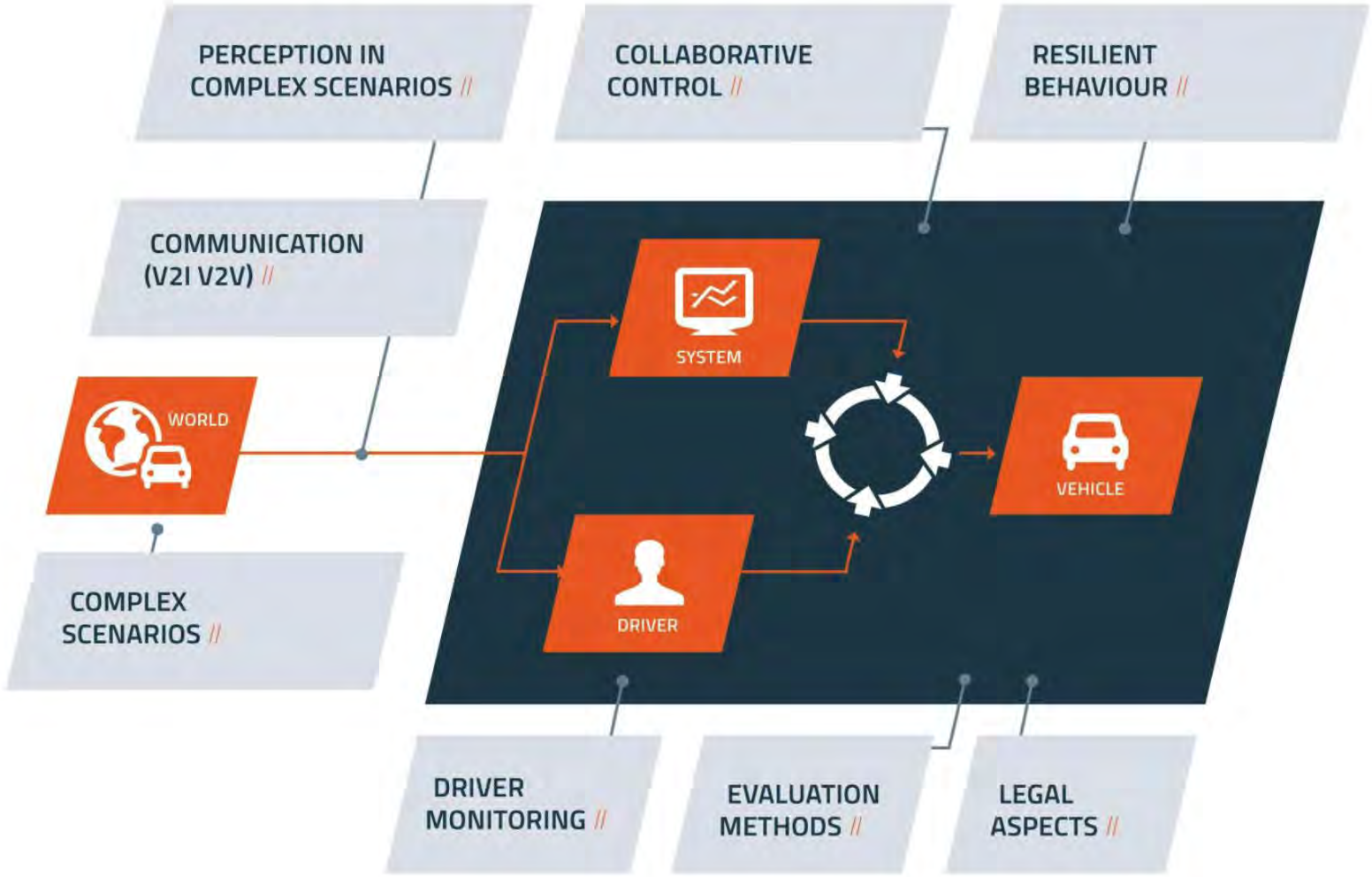
Her research interests include wireless security, network security, and IoT security. She is among the first to discover vulnerabilities of tire pressure monitor systems in modern automobiles and automatic meter reading systems.

Dr. Xu received the NSF Career Award in 2009. She has served on the technical program committees for several IEEE/ACM conferences on wireless networking and security, and she is an associated editor of EURASIP Journal on Information Security.

Table of Contents

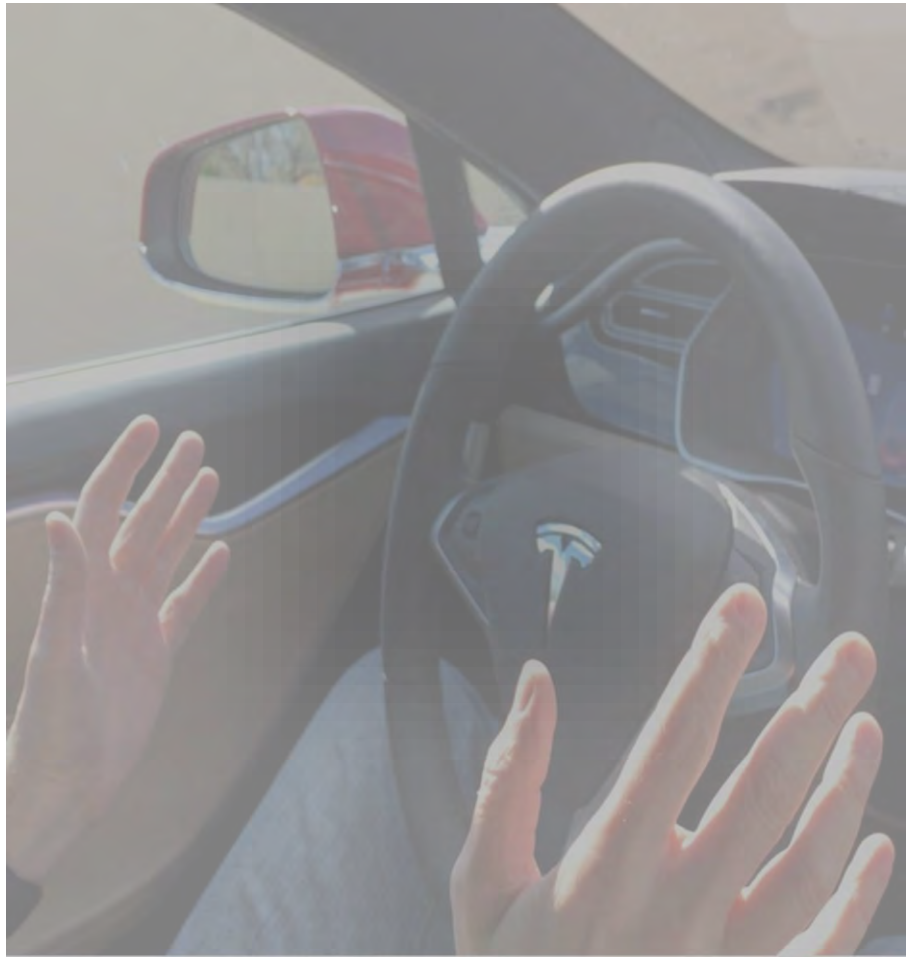
- Autonomous Vehicles
- Basics of automated driving
- Hacking autonomous cars by sensors
- Attacking ultrasonic sensors
- Attacking MMW Radars
- Attacking cameras
- Discussion

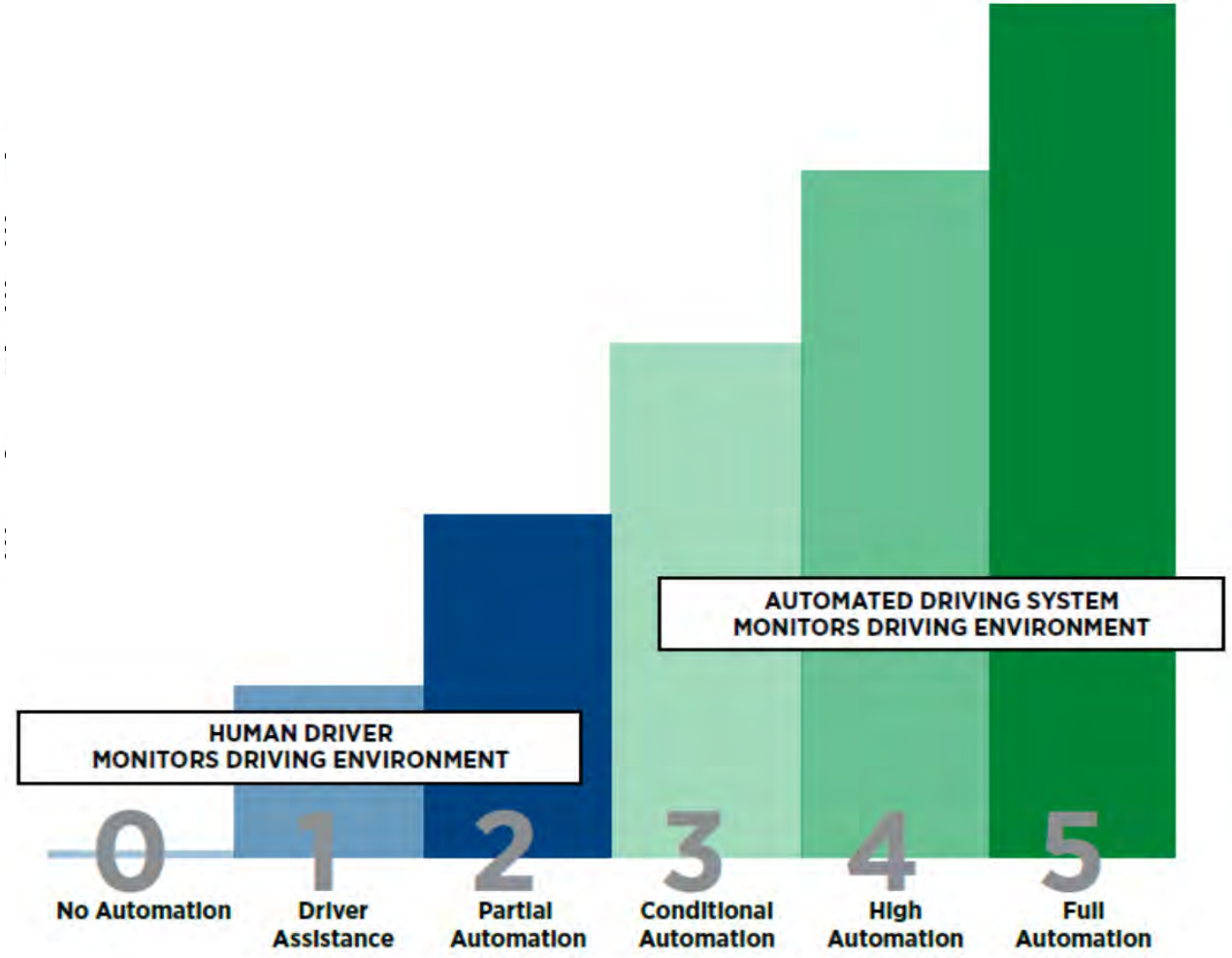
What is Autonomous Vehicle?



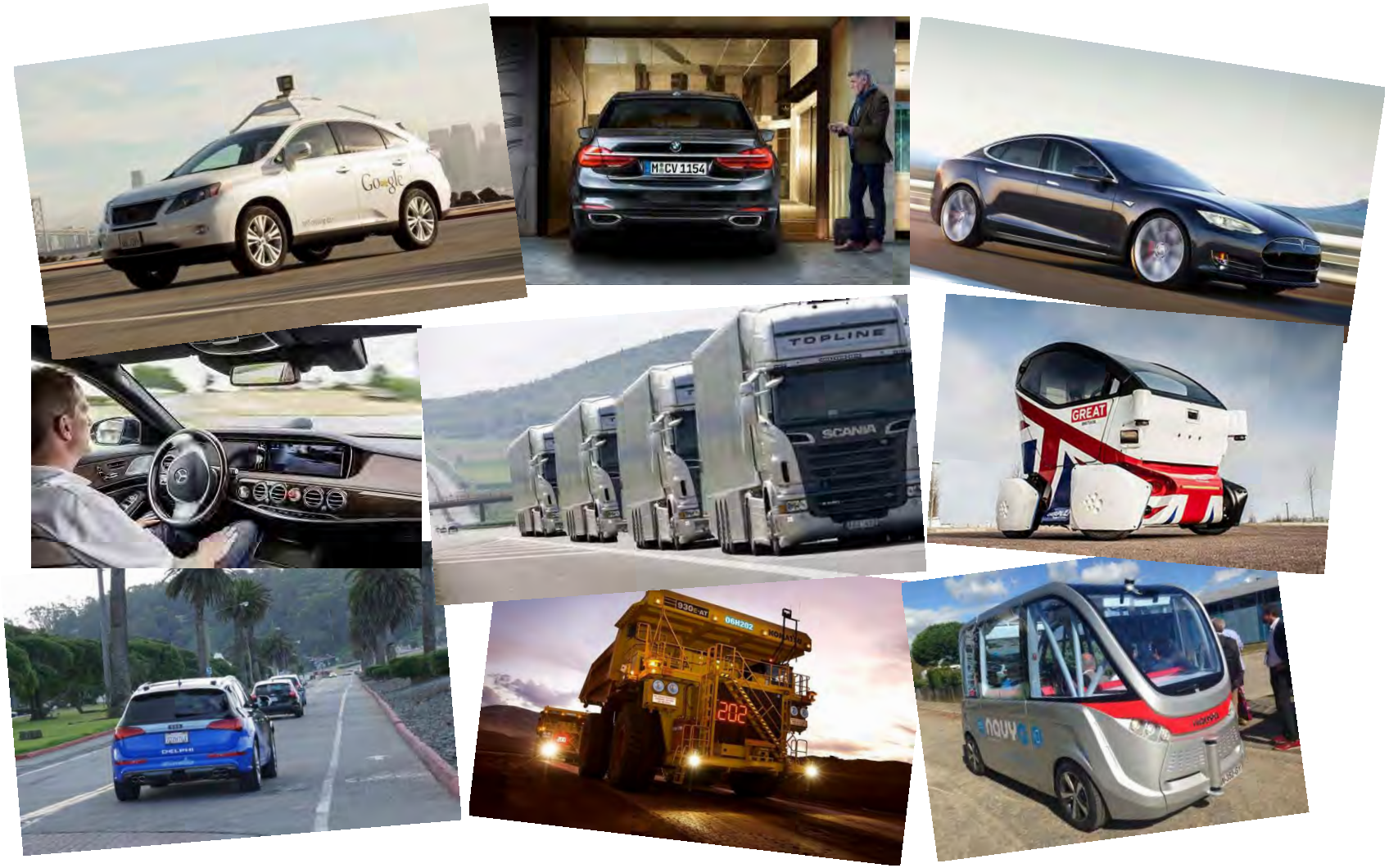
Source:Michael Aeberhard, BMW Group Research and Technology

Levels of Driving Automation

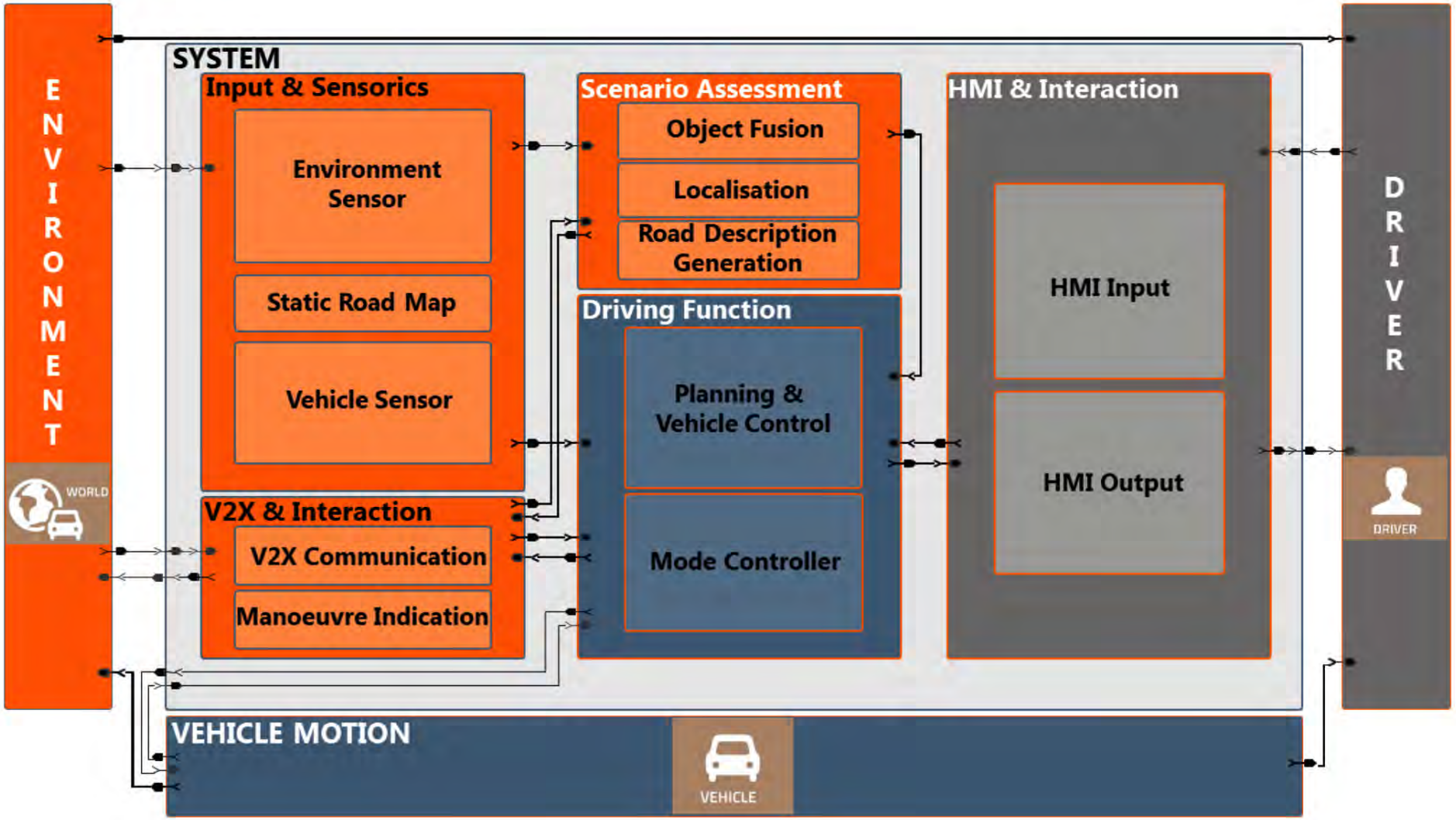




Connected Automated Vehicles

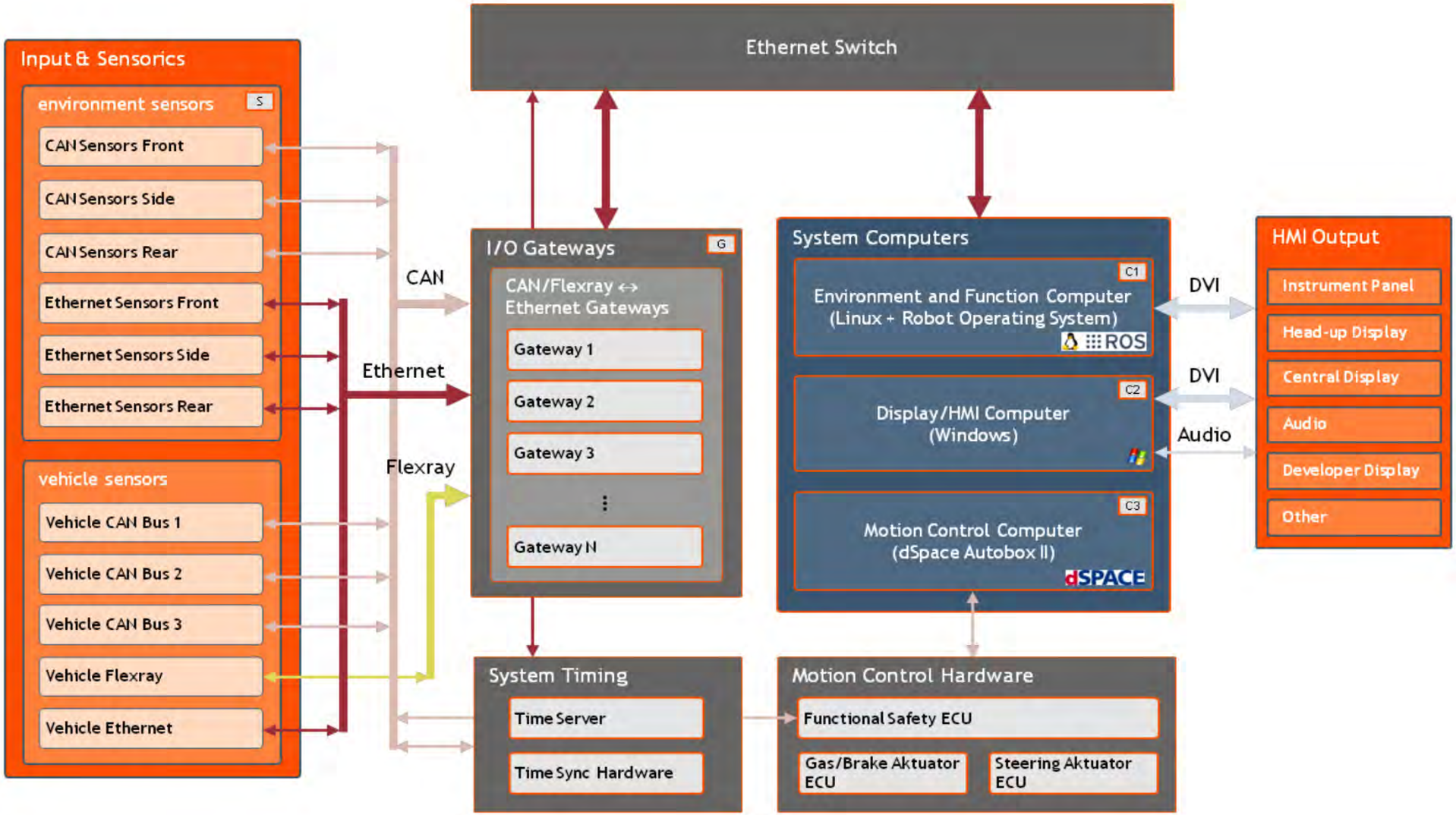


How can cars be Autonomous?



Source:Michael Aeberhard, BMW Group Research and Technology

Hardware Architecture



Source:Michael Aeberhard, BMW Group Research and Technology

Vehicle Sensors

Radar

Works in low light & poor weather, but lower resolution.

LiDAR

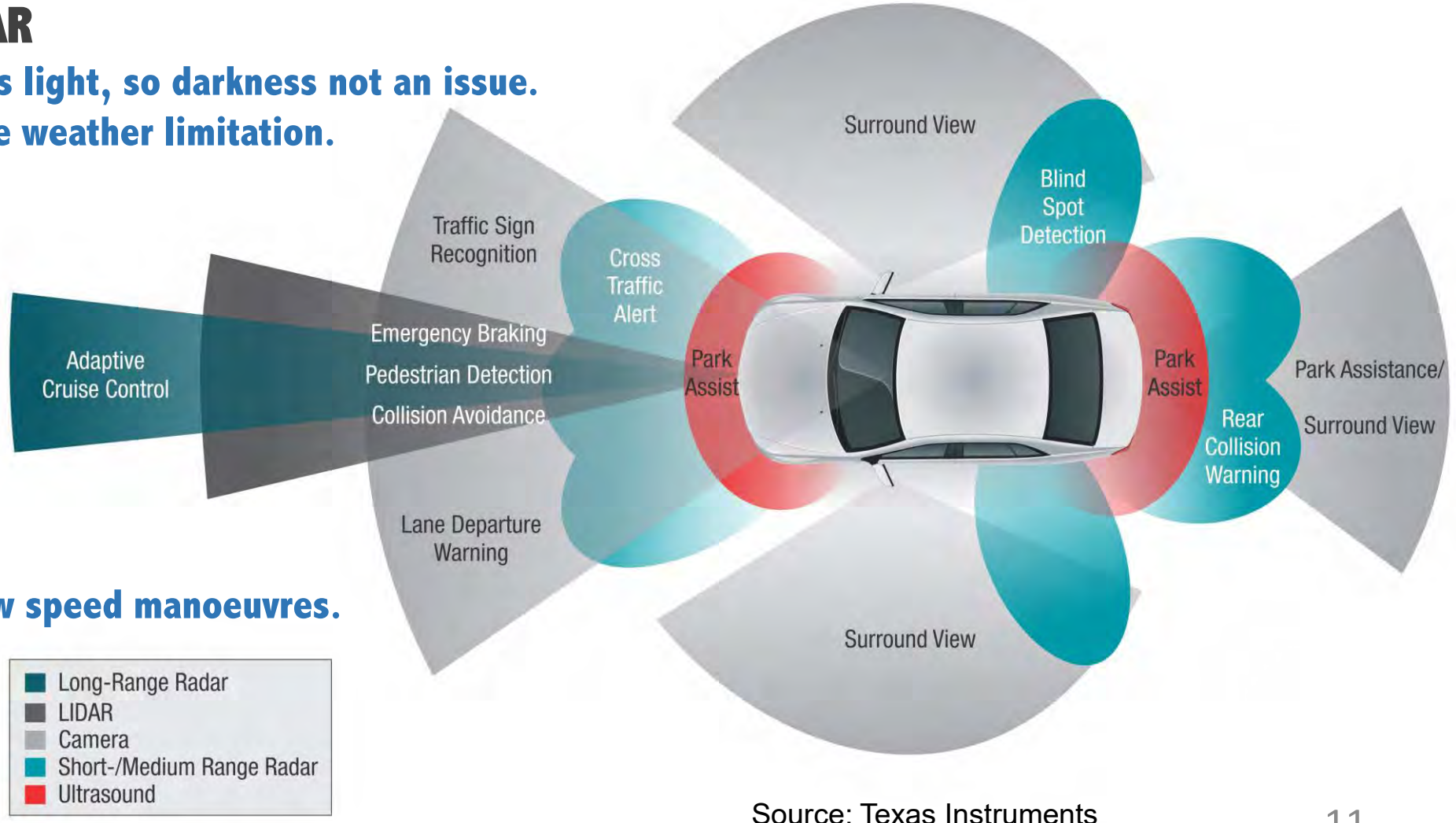
Emits light, so darkness not an issue.
Some weather limitation.

Camera

Senses reflected light, limited when dark.
Sees colour, so can be used to read signs, signals, etc.

Ultrasound

Limited to proximity, low speed manoeuvres.



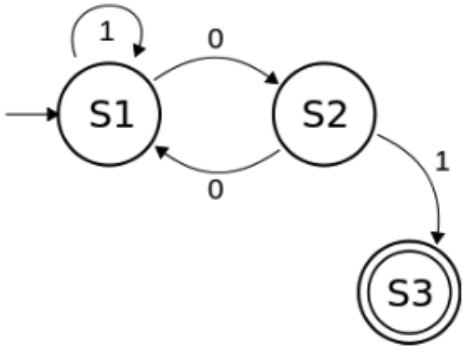
Source: Texas Instruments

Vehicle Controllers

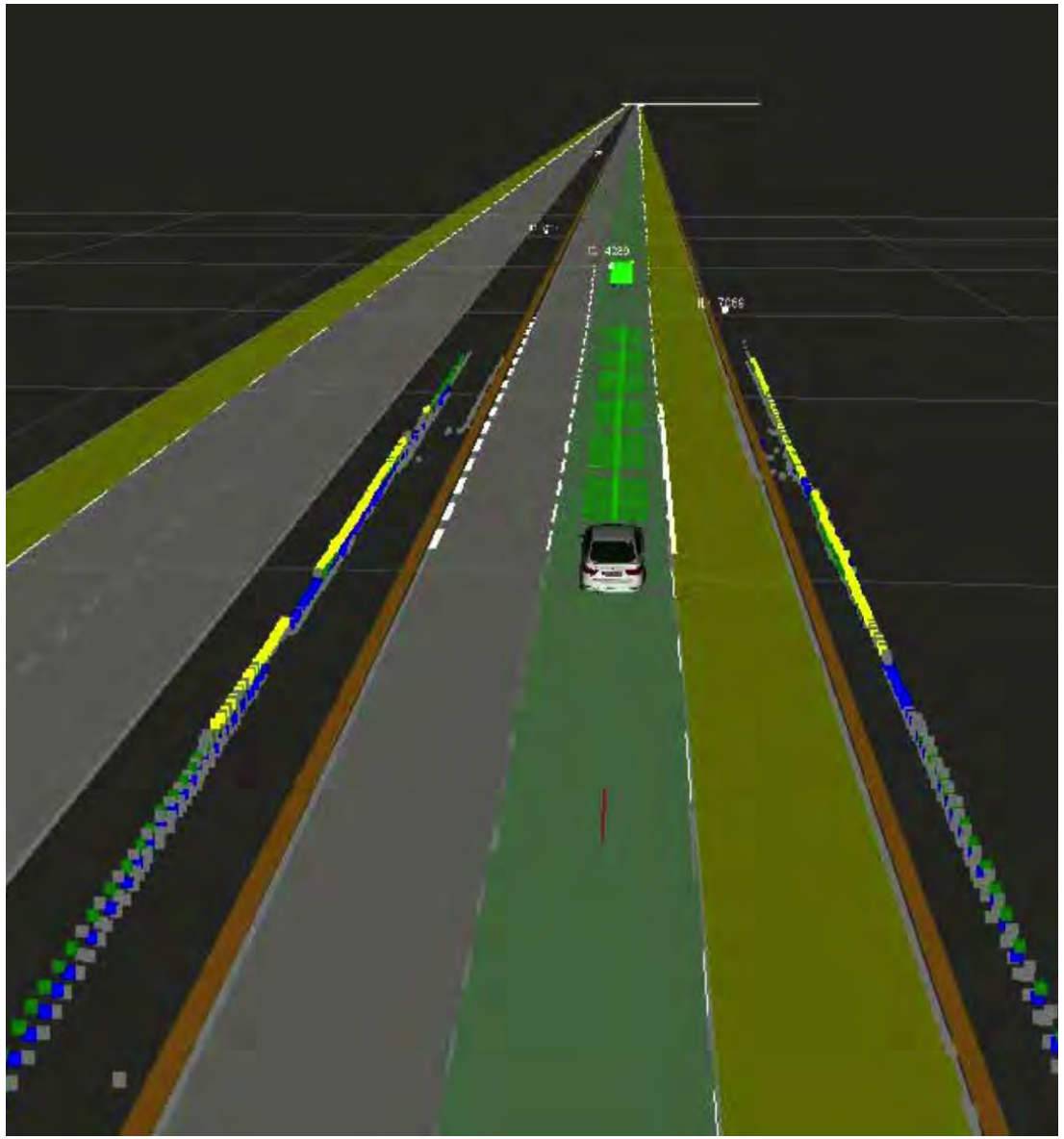
Autonomous System

■ Maneuver Planning

■ State Machine



■ Trajectory Planning



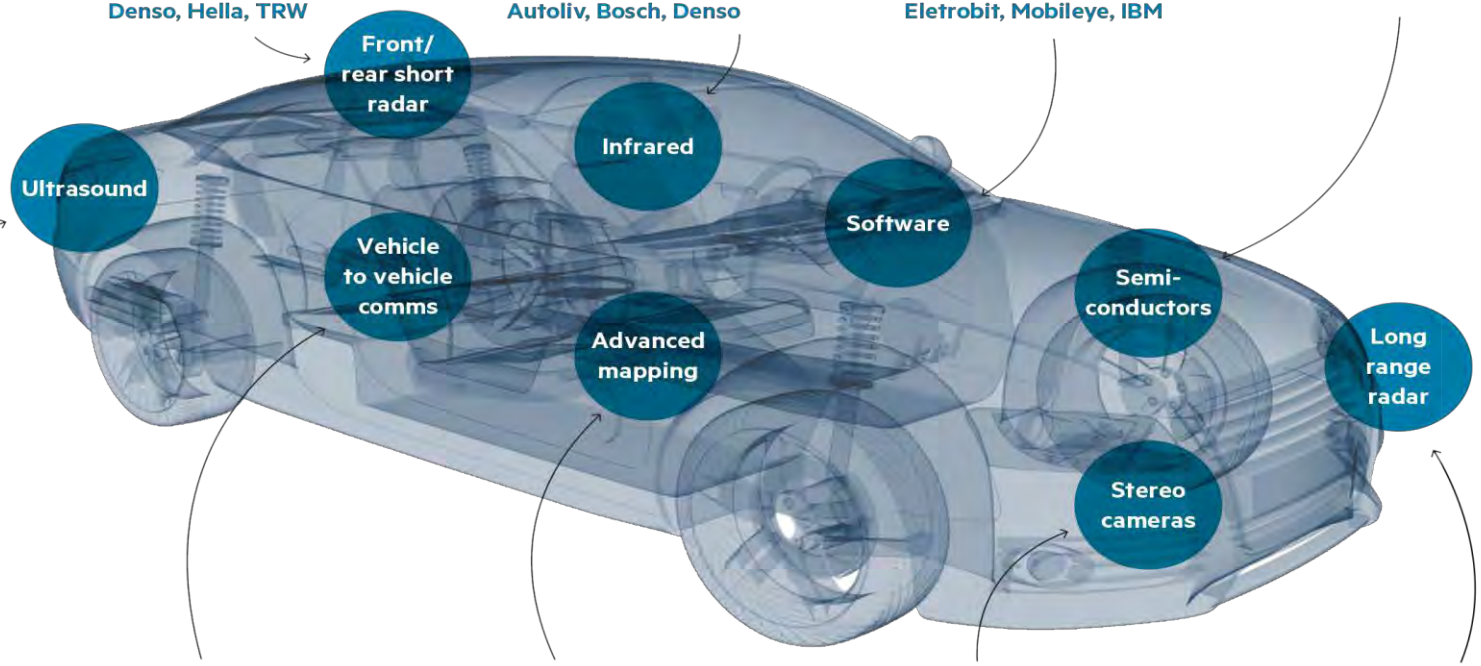
Source:Michael Aeberhard, BMW Group Research and Technology

Advanced Driver Assistance System (ADAS)

Advanced driver assistance systems

Carmakers are facing seismic change. Suppliers which were largely kept under the hood are set to grow in influence as the industry adds more and more autonomous features to vehicles

Suppliers listed in blue*



Detects close range objects to aid parking and avoid collision by using radio waves **Autoliv, Bosch, Continental, Delphi, Denso, Hella, TRW**

Enables in-car night vision systems that can detect objects further away than traditional headlights helping to avoid collisions at night **Autoliv, Bosch, Denso**

Integrates driver assistance functions; algorithms for every scenario **Carmakers, Tier-One suppliers, Google, Eletrobit, Mobileye, IBM**

Semiconductors underpin advanced electronic functionality **Renasas, Infineon, ST, TI, Freescale, NXP, Nvidia, Intel**

Used in front and rear parking sensors in modern cars. Will be adapted for assisted parking and short range pedestrian/obstacle detection **Bosch, Continental, Denso, Valeo**

Allows vehicles to communicate with each other **Autotalks, Codha Wireless**

For precise navigation **Google, TomTom, HERE (Nokia)**

Identifies both directional and distance information used in lane departure systems and traffic sign recognition **Autoliv, Bosch, Continental, Takata**

Seeks longer range objects for use in Adaptive Cruise Control systems **Autoliv, Bosch, TRW, Continental, Hella, Valeo**

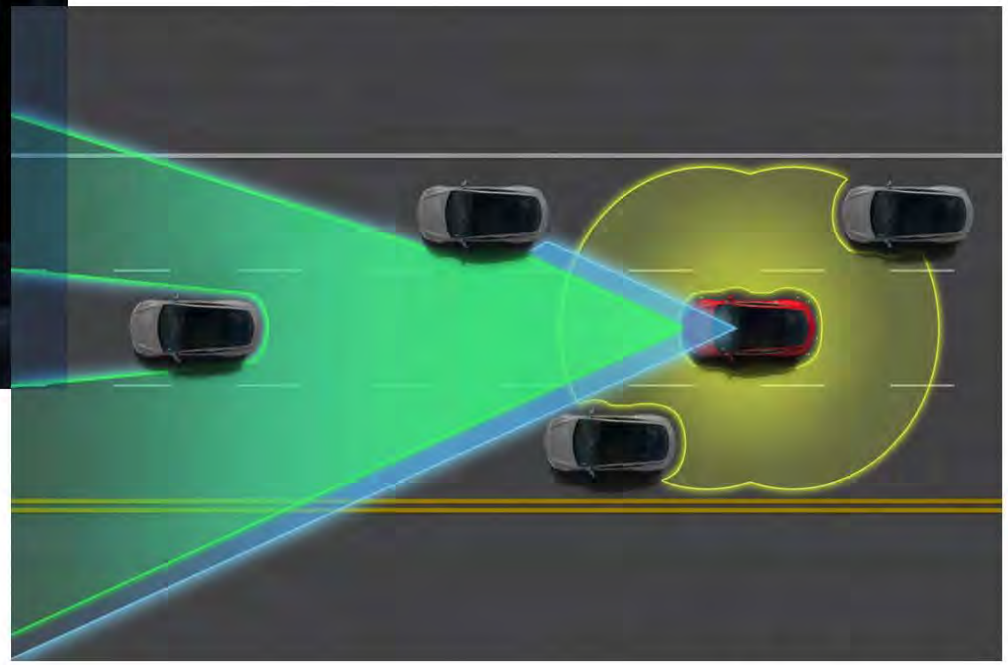
Sources: Exane BNP Paribas; Autoliv; Morgan Stanley; FT research *Lists of suppliers are not exhaustive Image: Cherezoff/Dreamstime FT graphic

ADAS Application

Demo of Tesla Model S Autopilot

"Tesla's Autopilot is a way to relieve drivers of the most boring and potentially dangerous aspects of road travel – but the driver is still responsible for, and ultimately in control of, the car……"

"Tesla announces new Autopilot feature"



Sources: www.teslamotors.com

How to Hack Sensors?

Sensors

Cameras

Blinding

MMW Radars

Spoofing

Jamming

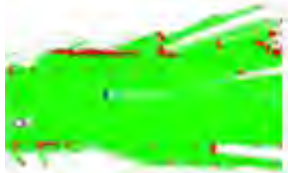
Ultrasonic Sensors

Spoofing

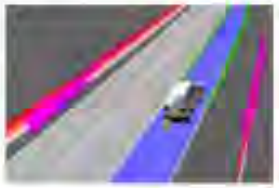
Jamming

Autonomous System

Representations and Fusion



Road Model and Localization



Situation Interpretation

Control

Display

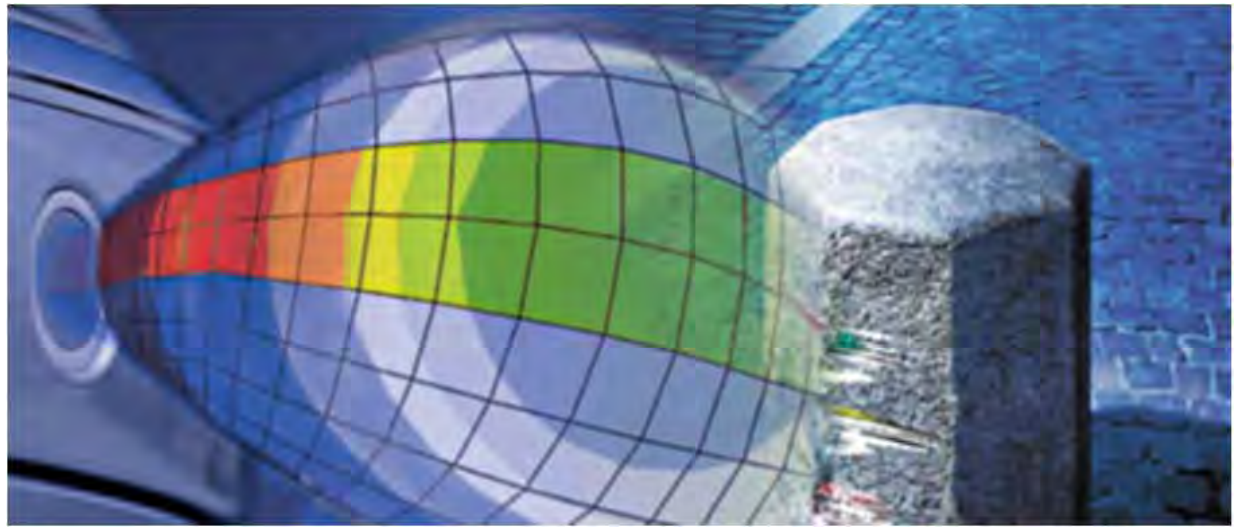
Attacking Ultrasonic Sensors

On Tesla, Audi, Volkswagen, and Ford

Ultrasonic Sensors

Proximity sensor

- **Parking assistance**
- **Parking space detection**
- **Self parking**
- **Tesla's summon**

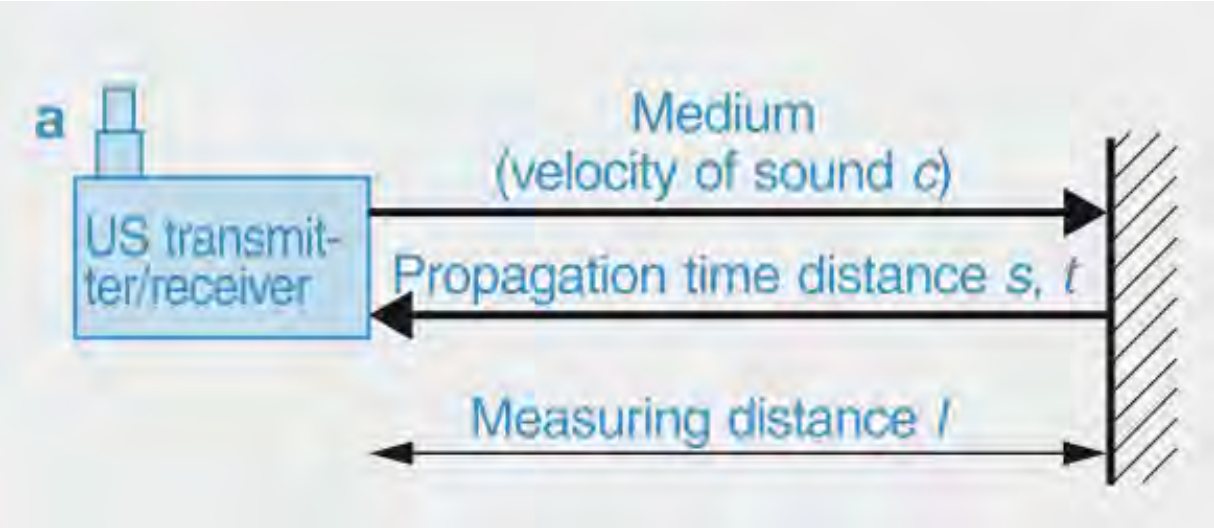


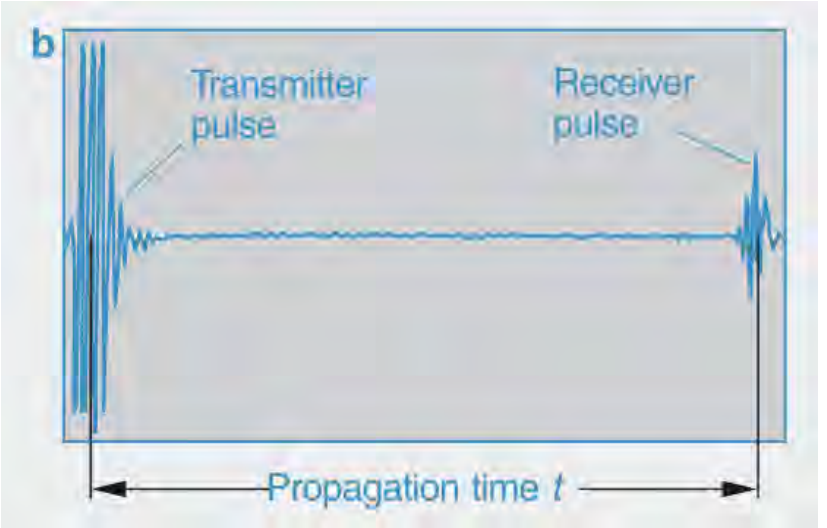
Parking Assistance

How do ultrasonic sensors work?

- **Piezoelectric Effect**
- **Emit ultrasound and receive echoes**
- **Measure the propagation time (Time of Flight)**
- **Calculate the distance** $d = 0.5 \cdot t_e \cdot c$

t_e : propagation time of echoes
c : velocity of sound in air





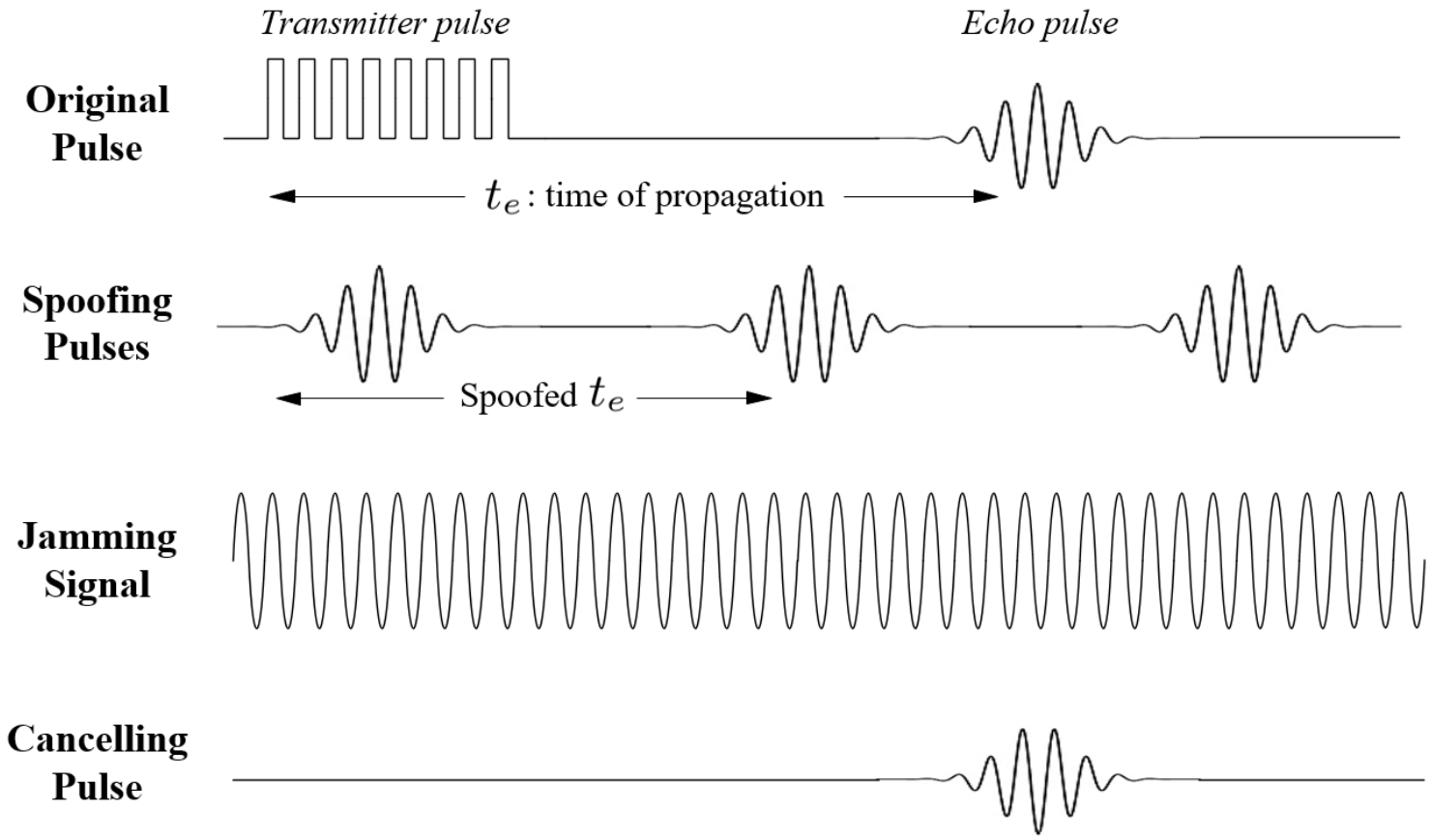
Attacking ultrasonic sensors

Attacks:

- **Jamming**
- **Spoofing**
- **Cancellation**

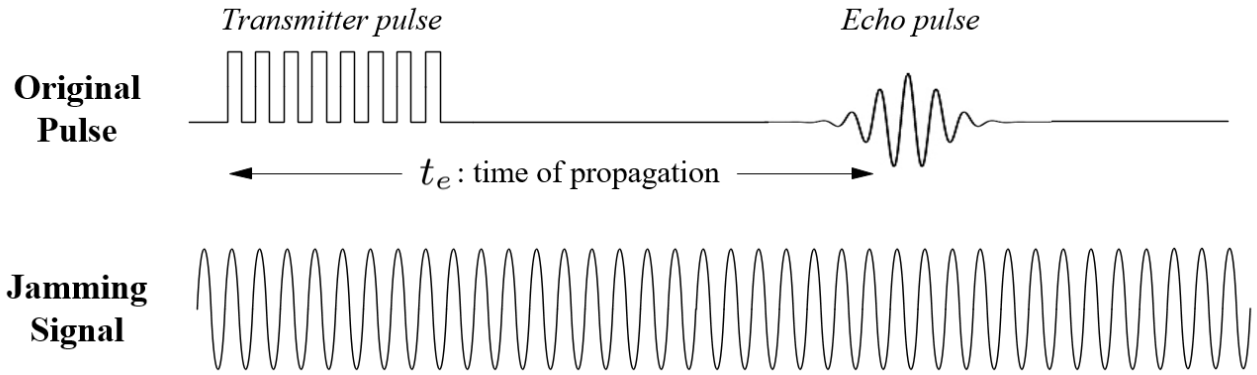
Equipment:

- **Arduino**
- **Ultrasonic transducer**



Jamming Attack

Known performance defect



Basic Idea:

- **Injecting ultrasonic noise to lower Signal to Noise Ratio (SNR)**
- **At resonant frequency (40 – 50 kHz)**

Experiment target:

- **8 stand-alone ultrasonic sensor modules**
- **Tesla, Audi, Volkswagen, Ford**

Jamming Attack - Setup

Car in figure:

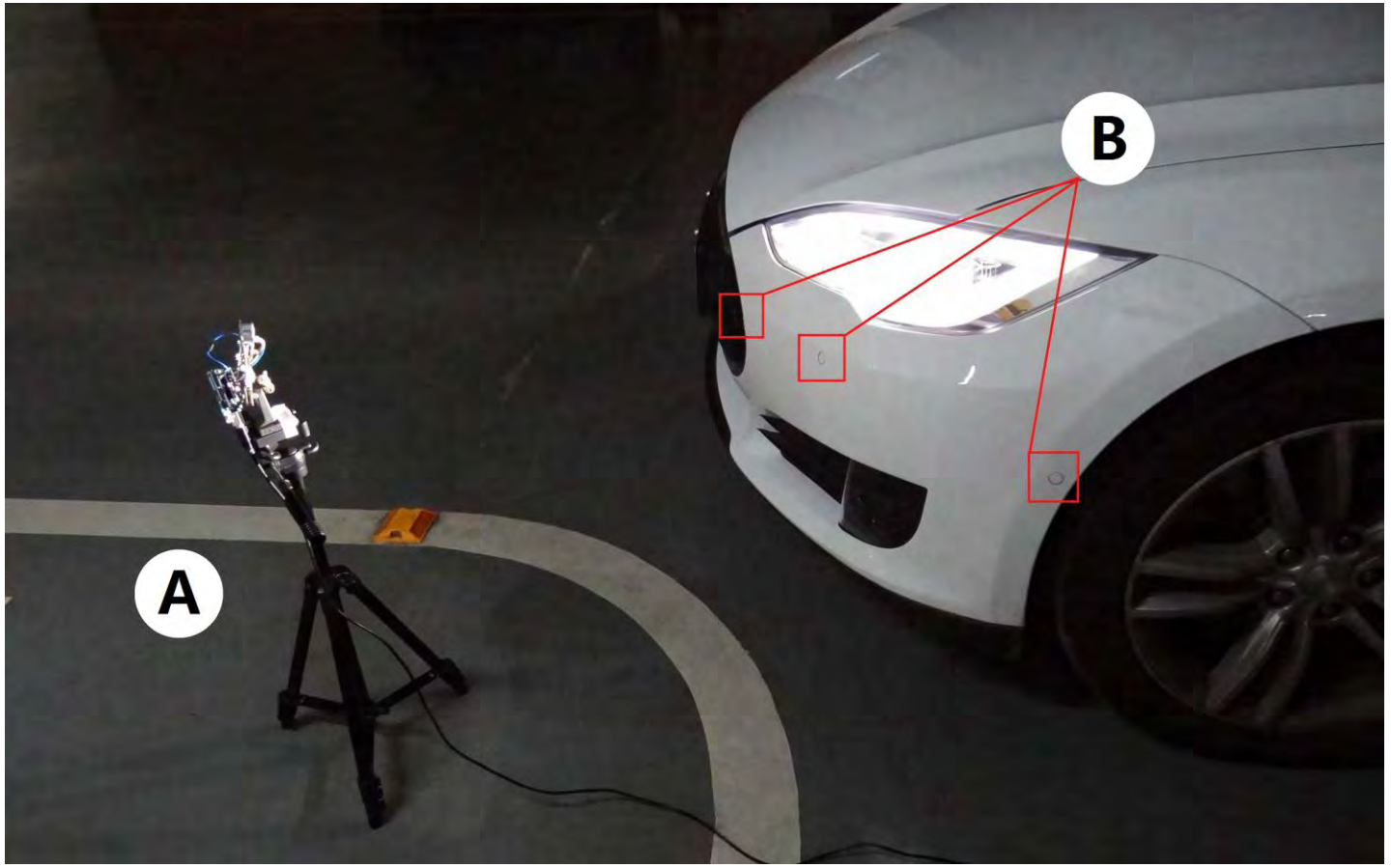
Tesla Model S

A:

Ultrasonic Jammer

B:

3 ultrasonic sensors on the left front bumper



Jamming Attack – Demo on Tesla

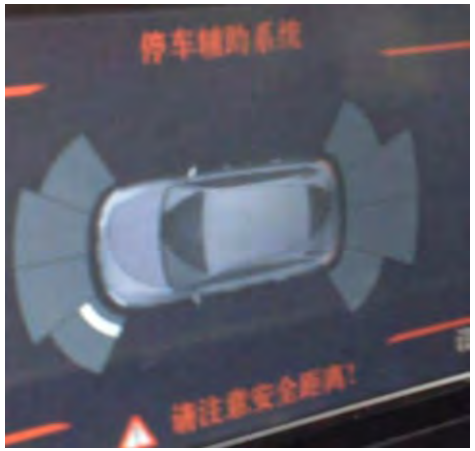
Jamming Attack – Demo on Audi

Jamming Attack – Results

- On ultrasonic sensors
- On cars with parking assistance
- On Tesla Model S with self-parking and summon

Tesla Normal

Tesla Jammed



Audi Normal

Audi Jammed

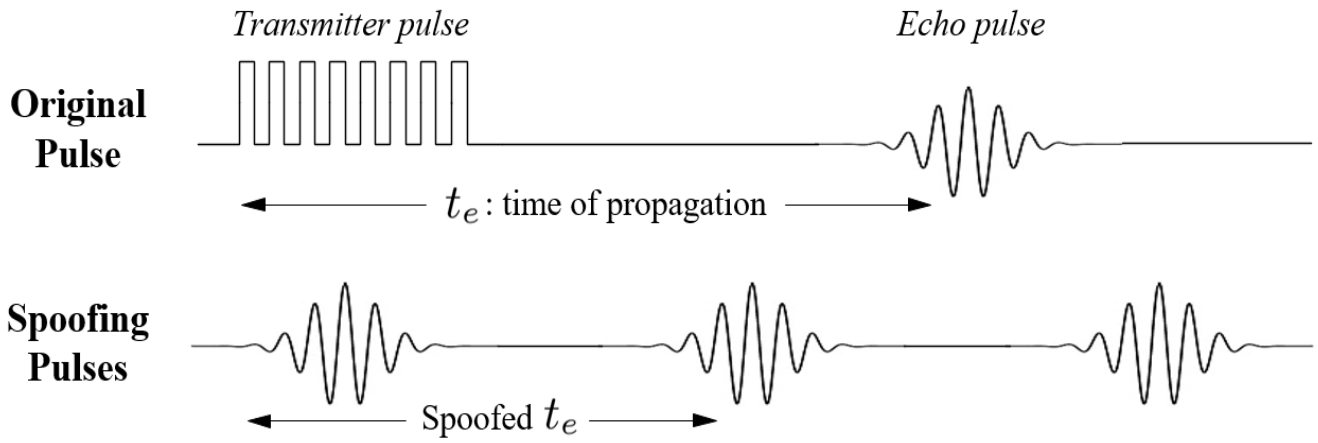
Spoofing Attack

Basic Idea

- Transmitting ultrasonic pulses with similar pattern
- Timing matters!

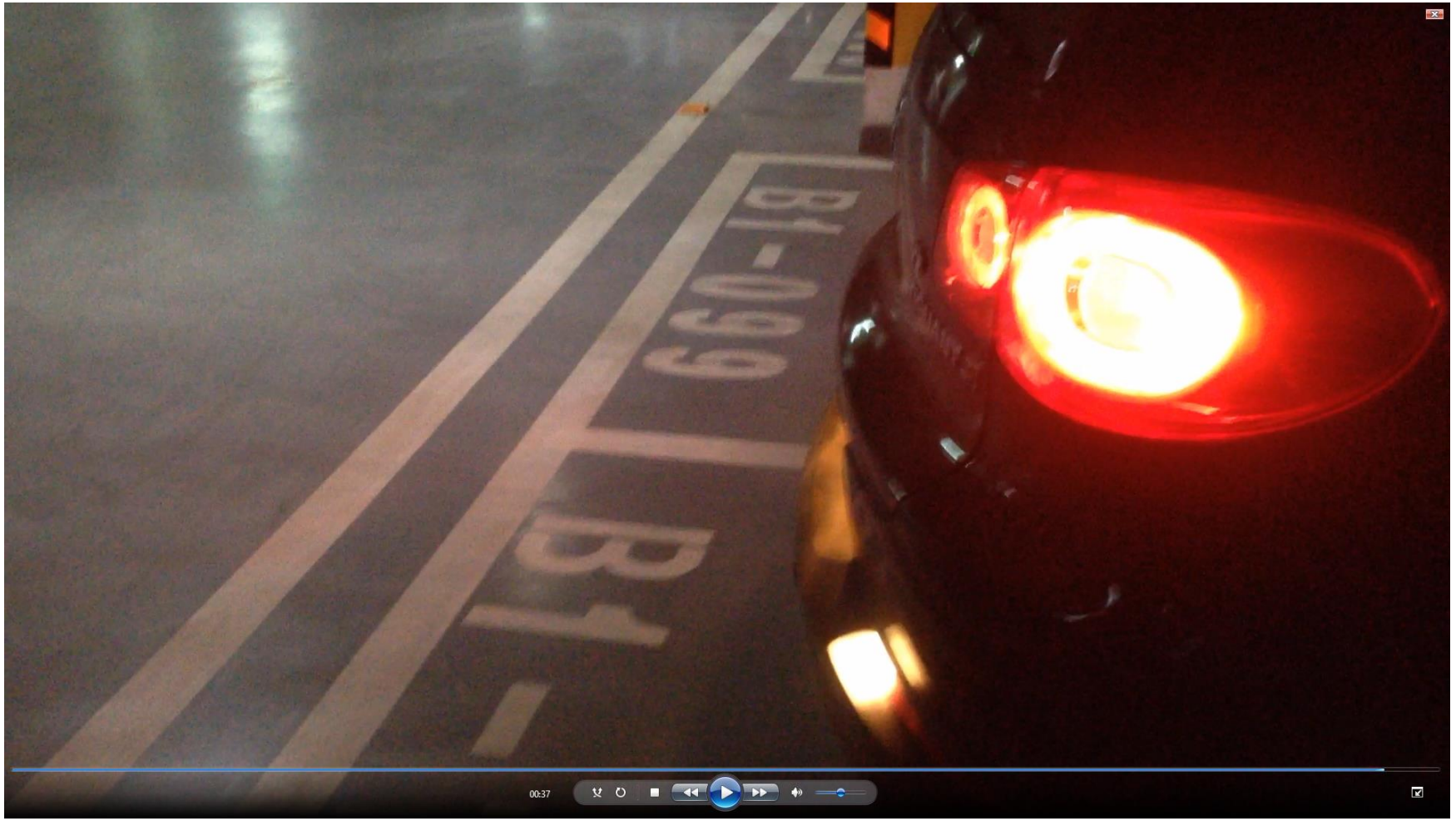
Difficulty

- Only the first justifiable echo will be processed



Spoofing Attack – Demo on Tesla

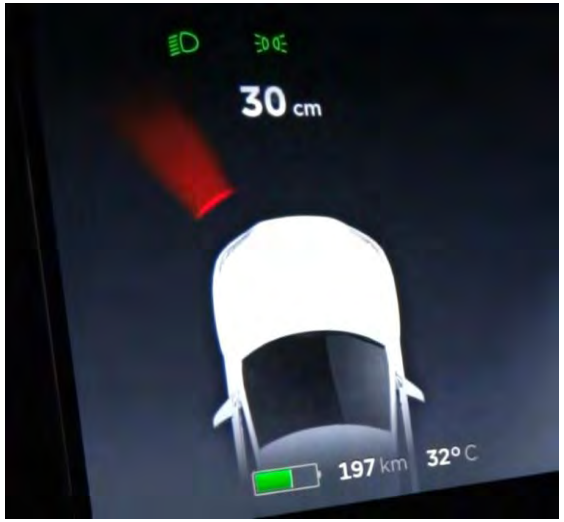
Spoofing Attack – Demo on Volkswagen



Spoofing Attack - Results

- On ultrasonic sensors
- On cars with parking assistance

Tesla Normal

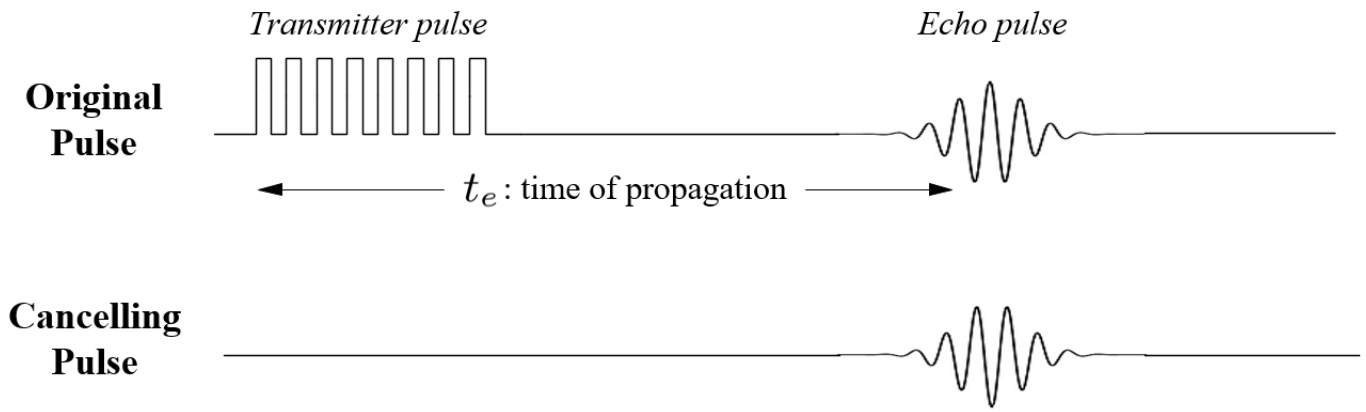


Tesla Spoofed

Audi Spoofed

Acoustic Quieting

- Cloaking
  - Sound absorbing materials
- Acoustic Cancellation
  - Cancel with sound of reverse phase
  - Minor phase and amplitude adjustment



Attacking Millimeter Wave Radars

On Tesla Model S

Millimeter Wave Radar

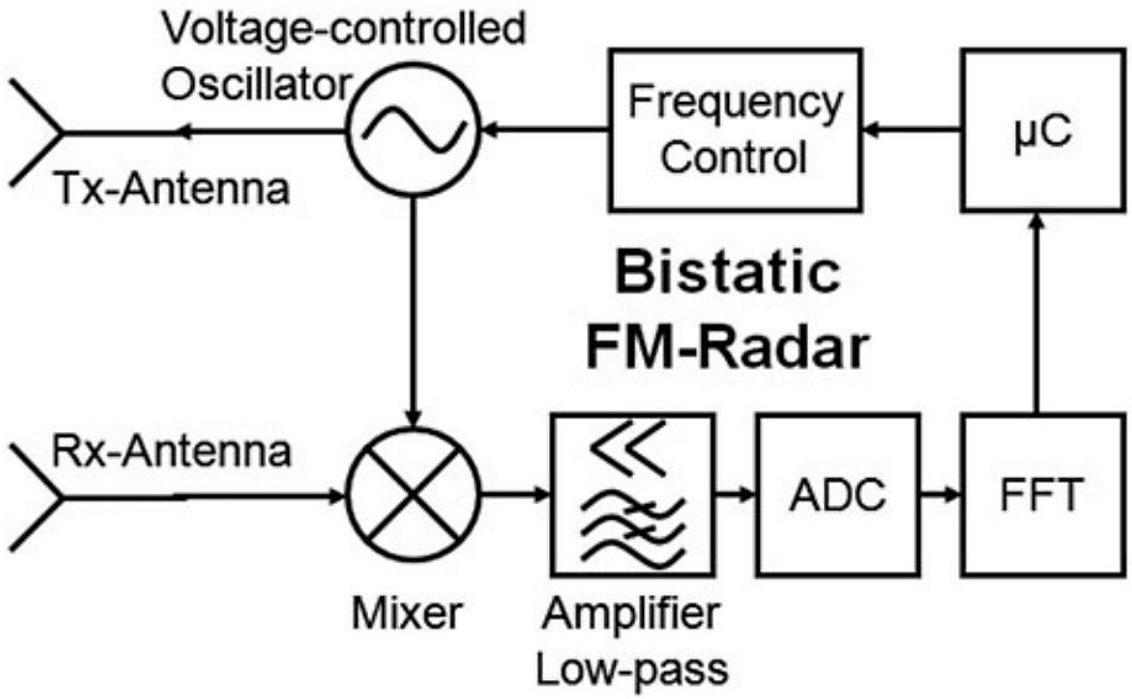
Short to long range sensing

- **Adaptive Cruise Control (ACC)**
- **Collision Avoidance**
- **Blind Spot Detection**

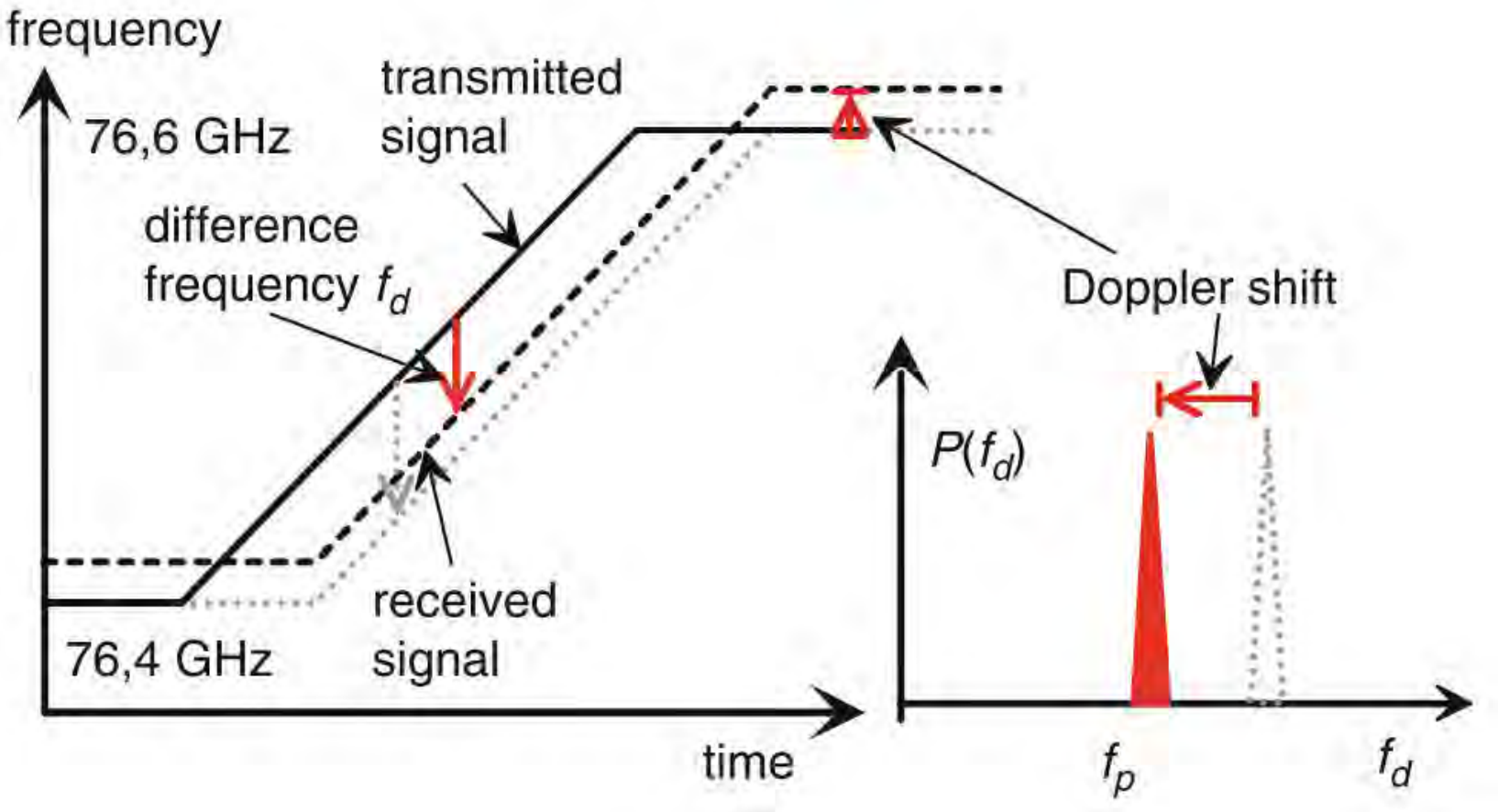
Construction of the Bosch RADAR sensors MRR and LRR3 (Source: Bosch)

How do MMW Radars work?

- Transmit and receive millimeter electromagnetic waves
- Measure the propagation time
- **Modulation**
  - Amplitude
  - Frequency (**FMCW**)
  - Phase
- Doppler Effect
- Frequency Bands:
  - 24 GHz
  - **76-77 GHz**



Frequency Modulated Continuous Wave (FMCW)



Attacking MMW Radars & Setup

Attacks:

- **Jamming**
- **Spoofing**
- **Relay**

Equipment:

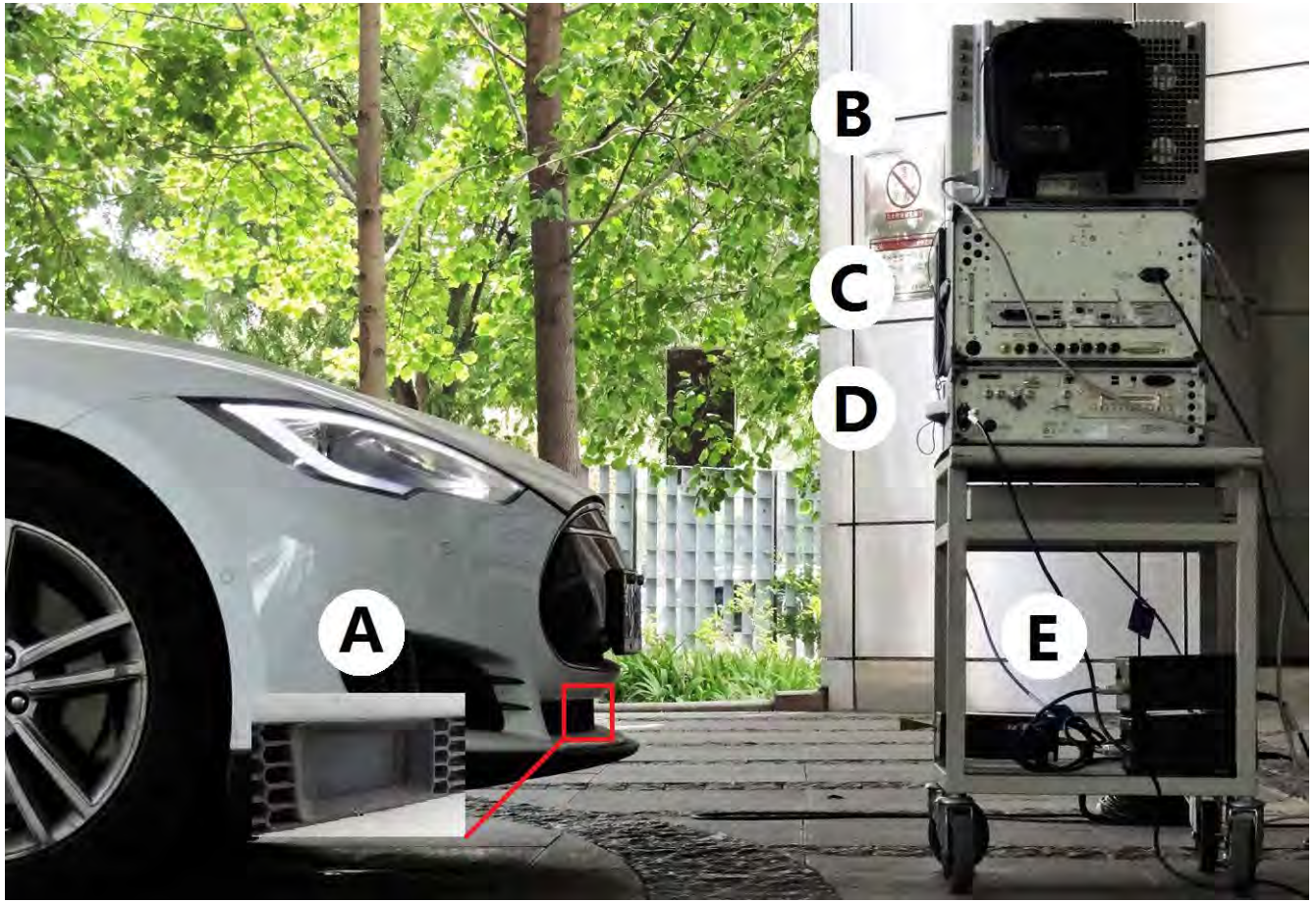
Signal analyzer (C)

Harmonic mixer (E)

Oscilloscope (B)

Signal generator (D)

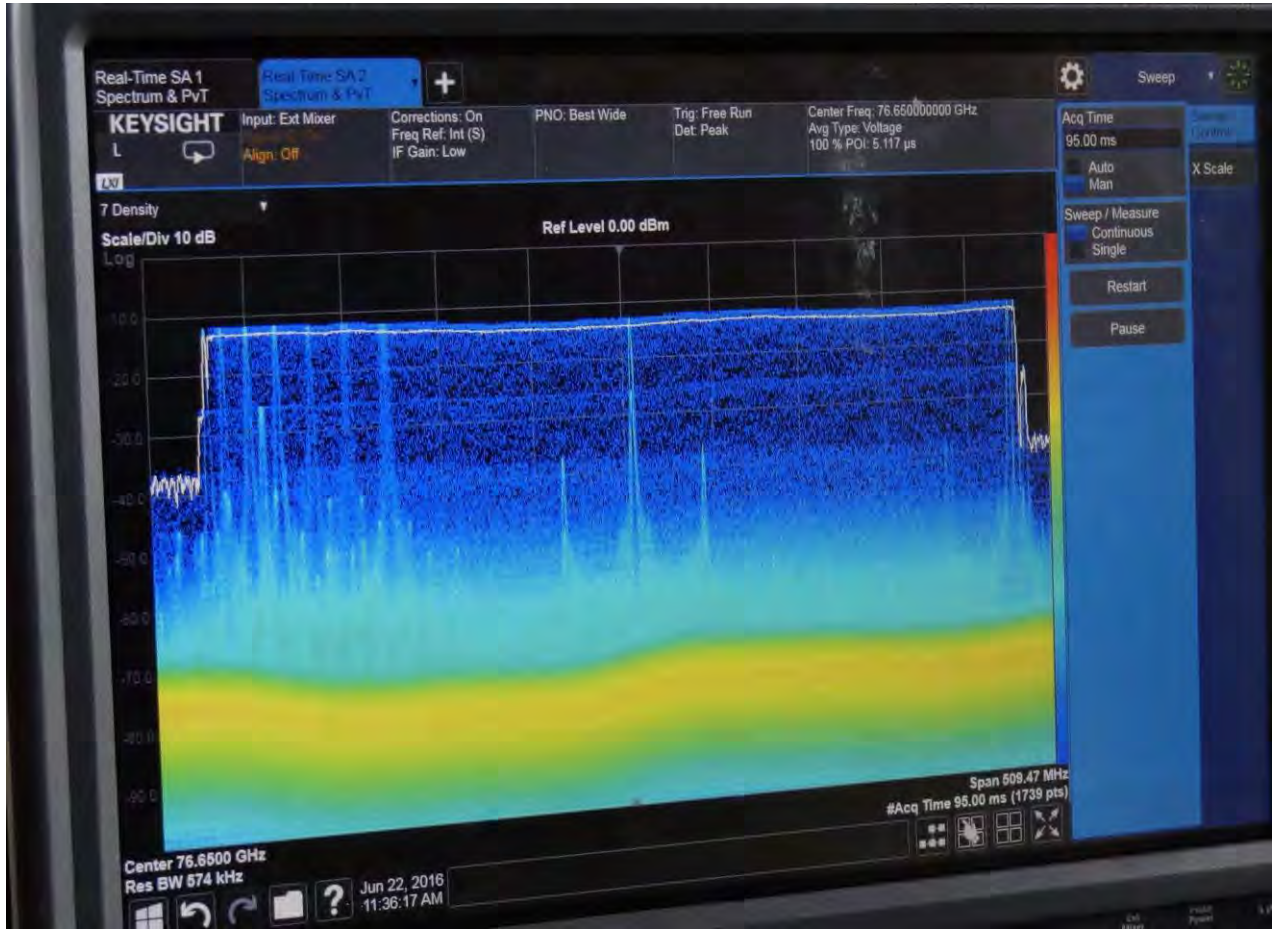
Frequency multiplier (E)



Attacking MMW Radars - Signal Analysis

- Center frequency: 76.65 GHz
- Bandwidth: 450 MHz
- Modulation: FMCW

…



Attacks on MMW Radar

Jamming Attack

- Jam radars within the same frequency band, i.e., 76 - 77 GHz

Spoofing Attack

- Spoof the radar with similar RF signal

Relay Attack

- Relay the received signal

Attacking MMW Radars - Results

- **Jamming: evaporate detected object**
- **Spoofing: tamper with object distance**

(a) Drive gear.

(b) Autopilot.

(c) Jammed.

Attacking MMW Radars – Demo on Tesla

Attacking Cameras

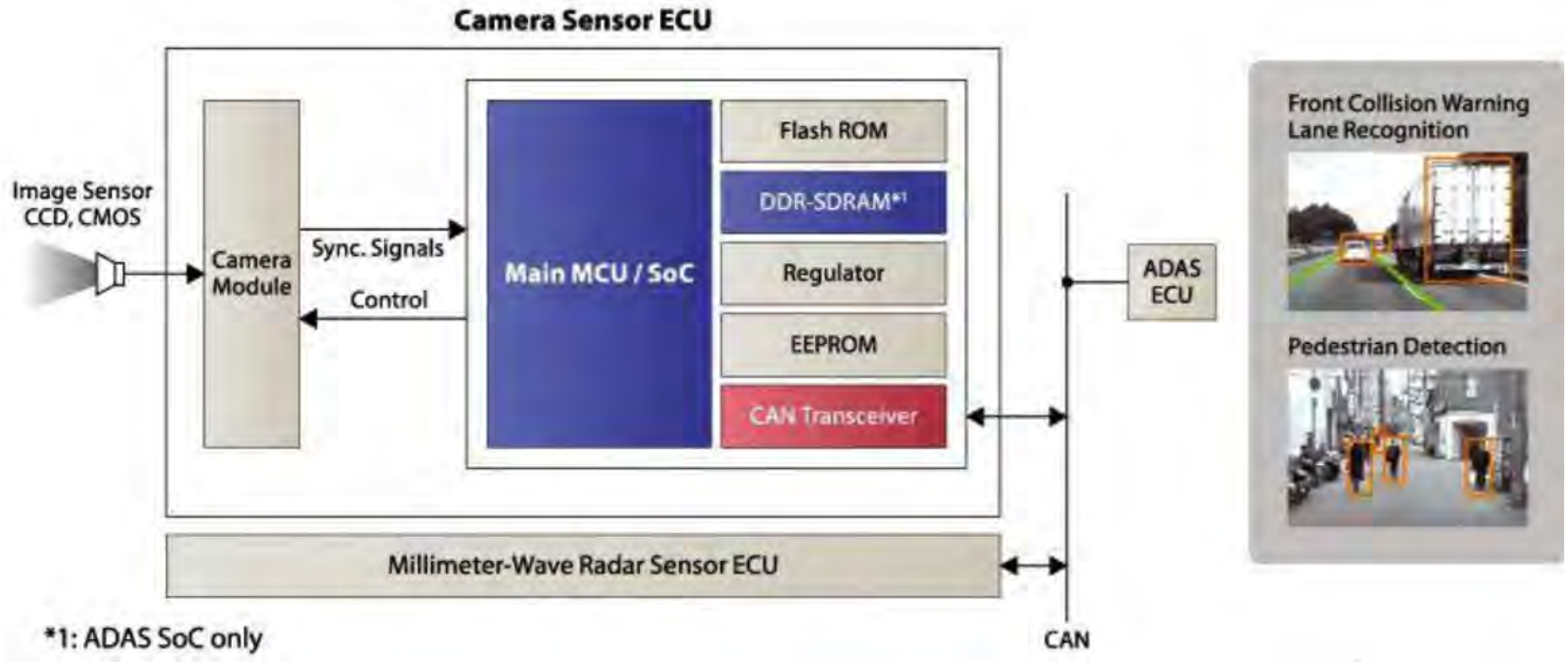
On Mobileye, Point Grey, and Tesla Model S

Automotive Cameras

Computer vision

- **Lane departure warning/keeping**
- **Traffic sign recognition**
- **Parking assistance**

How do automotive cameras work?



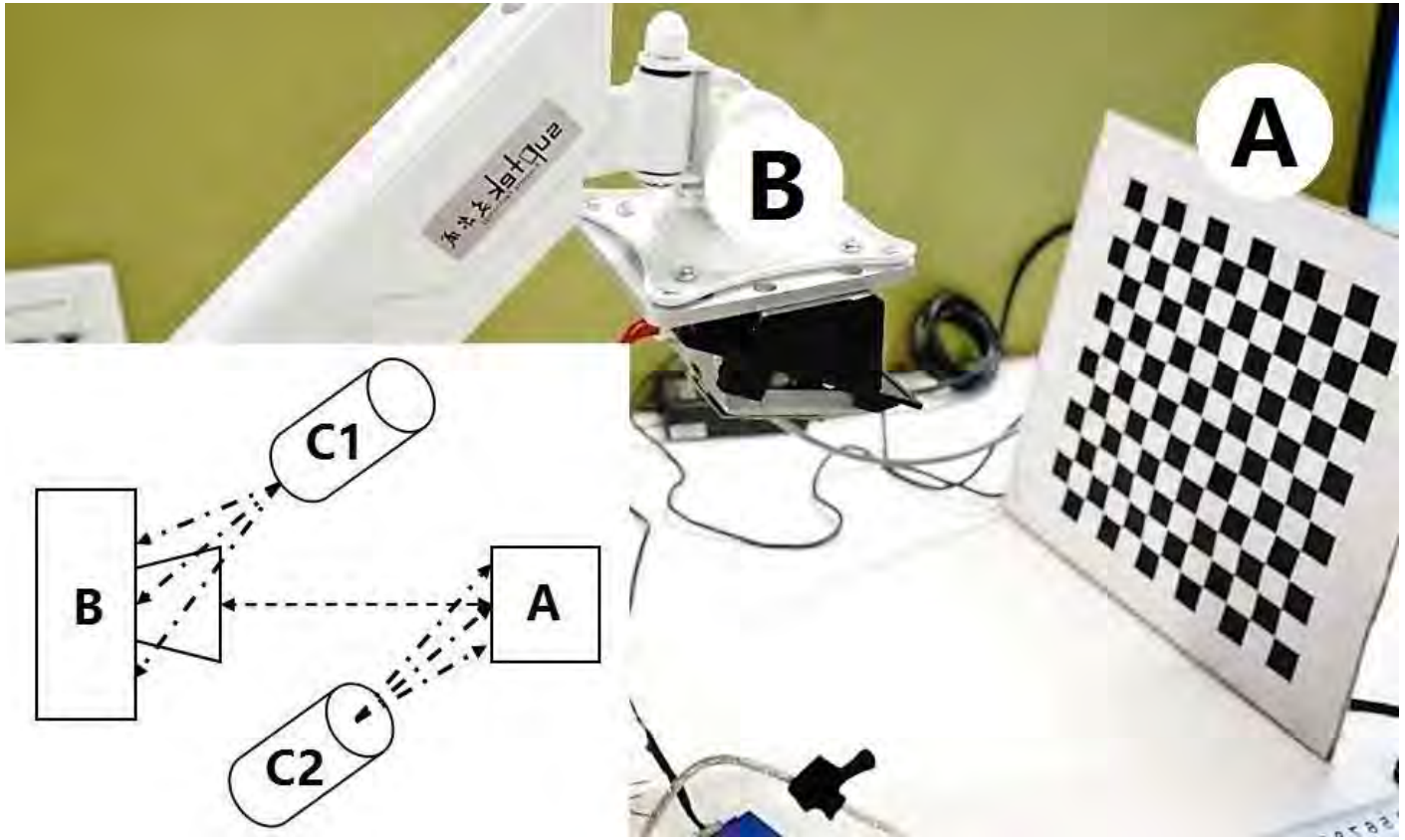
Attacking Cameras - Setup

Attack:

- **Blinding**

Equipment:

- **LED spot**
- **Laser**
- **Infrared LED spot**

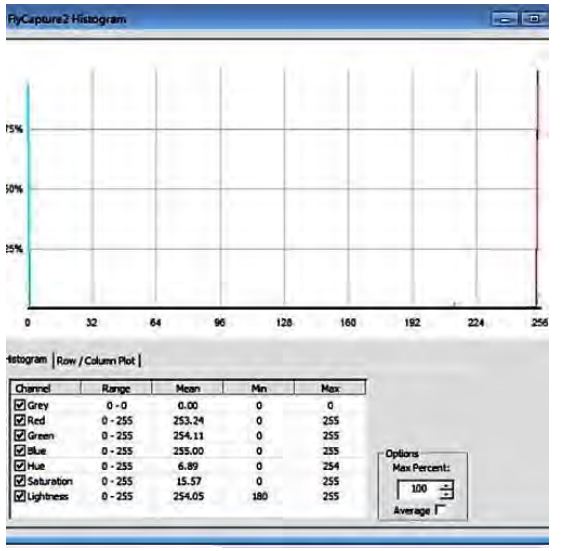


Attacking Cameras – Results with LED spot

- **Part or total blinding**

LED toward the board

LED toward camera

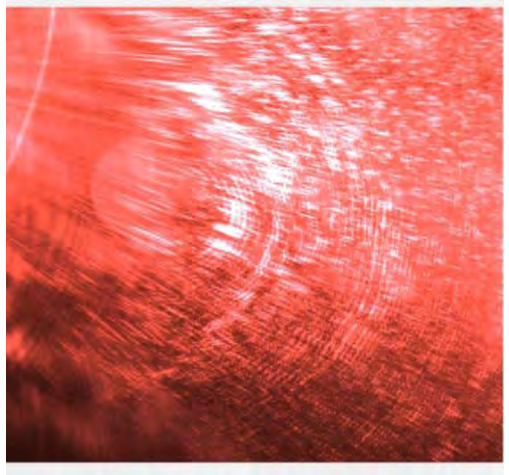


Tonal Distribution

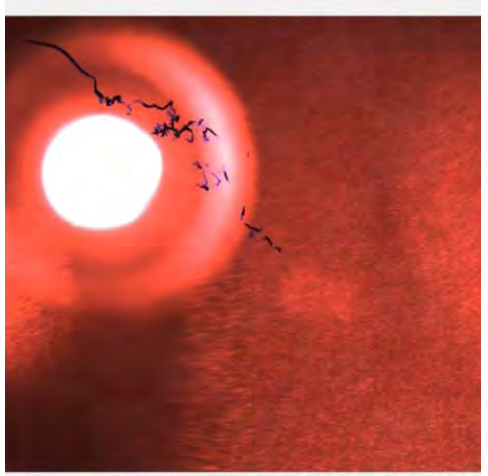
Attacking Cameras – Results with Laser

- Part or total blinding
- Permanent damage

Fixed beam



Wobbling beam



Damage caused

Damage is permanent

Discussion

- Attack feasibility
- Countermeasures
- Limitations & Future work

Conclusions and Takeaway messages

- **Realistic issues** of automotive sensor security
- Big **threat** to autonomous vehicles (present and future)
- Attacks on **ultrasonic sensors**
- Attacks on **MMW Radars**
- Attacks on **cameras**
- Attacks on **self-driving cars**

Questions and Answers

Jianhao Liu liujianhao@360.cn
Chen Yan yanchen@zju.edu.cn
Wenyuan Xu wyxu@cse.sc.edu