# Automotive Cybersecurity: An Introduction


- Rita M. Barrios, Ph.D.
- Associate Director – Vehicle Cyber Institute
- Adjunct Professor – Vehicle Cyber Engineering
- Sr. Cybersecurity Engineer Bosch Automotive

# What is Cybersecurity?

# What is Cybersecurity?

**Cybersecurity is the protection of Internet Connected, Computer-based Systems and their components (hardware, software, data, & people) against UNAUTHORIZED information disclosure, transfer, modification, or destruction, whether accidental or intentional.**

# CIA:
# Confidentiality, Integrity, & Availability

- **Confidentiality**: Ensuring critical information is accessible to only those AUTHORIZED to have access.
- **Integrity**: Software, Data, Hardware is complete and free from UNAUTHORIZED modifications
- **Availability**: Ensuring the system (hardware, software, & data) are usable as intended, in their intended environment

# Authentication vs. Authorization

- Authentication: Ensuring that the identity of the entity can be verified to True
- Authorization: Ensuring that an Authenticated entity has access to only those components that are needed to complete an assigned task

# Authentication

Entities can be human or electronic

Uses Cryptography functions

Methods: Passwords, Tokens, Digital Signatures & Certificates, Biometrics, etc.

**Strong Authentication**:
Ability to validate 2 of the following characteristic

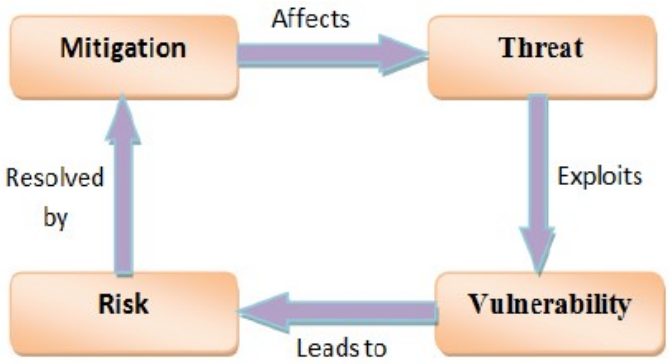
# Vulnerability, Threats & Risk

**Threat**: acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.

**Vulnerability**: a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system: Network, Operating Systems, Hardware, Software & Humans

**Risk**: the probability of exposure or loss resulting from a cyber attack or data breach: Loss can be tangible (e.g., money) or intangible (e.g., reputation)


**Vulnerabilities and Threats are mitigated by countermeasures that reduce Risk**



# Threat Actors

- Who are these hackers?
  - Individuals (significant time, varied expertise, limited $ & capability)
  - Corporate (moderate time, high expertise, moderate $ & capability)
  - Universities (moderate time & $, high expertise, high capability)
  - Terrorists (moderate time, varied expertise, moderate $ & capability)
  - Nation states (significant time, high expertise, high $ & capability)
- Hacking Goals
  - Fame, notoriety, revenge
  - Economic gain – e.g., unlock hidden functionality; access IP/content
  - Terrorism - e.g., disrupt  a city at rush hour; remove truck from service
- Hacking consequences
  - Brand damage – loss of customer confidence in products/systems
  - Liability – legal actions (criminal & civil)
  - Economic loss – recalls, replacements, repairs, future sales, fines
  - Loss of Life – vehicle crash, product malfunction

# Why Does it Matter?

# Four Factors to Consider

- Technology
  - What are we securing and **why** – not everything needs to be secured
- Economics of the stakeholders (Victim & Attacker)
  - Motivation: What do they have to gain or loose
- Social Influence
  - Public Perception of the Stakeholders
- Public Policy
  - Regulations, Standards, Laws

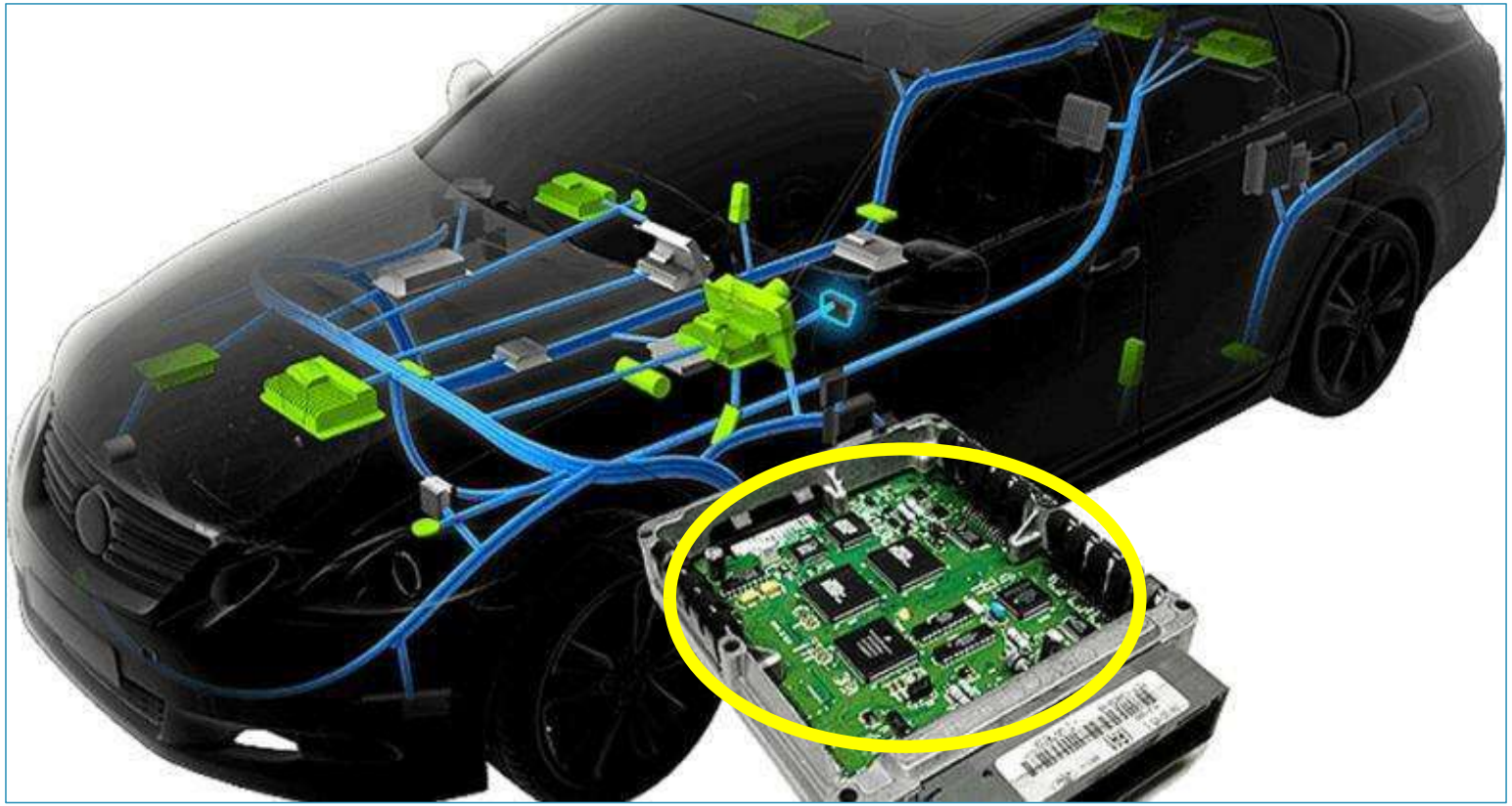
A quick overview…

# Automotive Cybersecurity

# A Computer on Wheels…


Motherboard, (2015), "How to Hack a Car: Phreaked Out" (Episode 2)

# Electronic Control Units (ECU)



# The Software Defined Vehicle

**787 Dreamliner**

**7+ Million LoC**

**Ford F150 Lightning EV**

**130+ Million LoC**

**F22 Raptor**

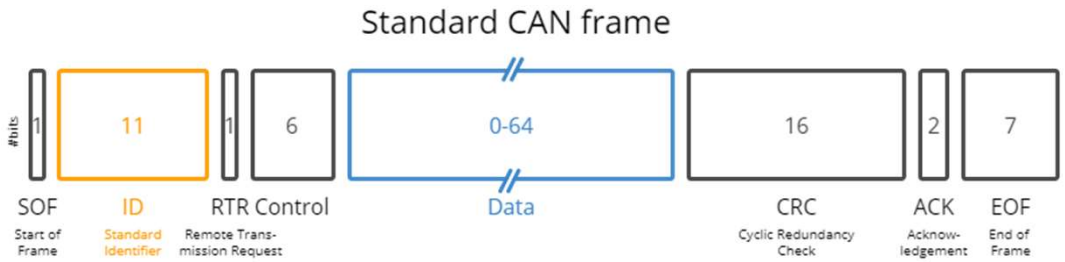
**2+ Million LoC**

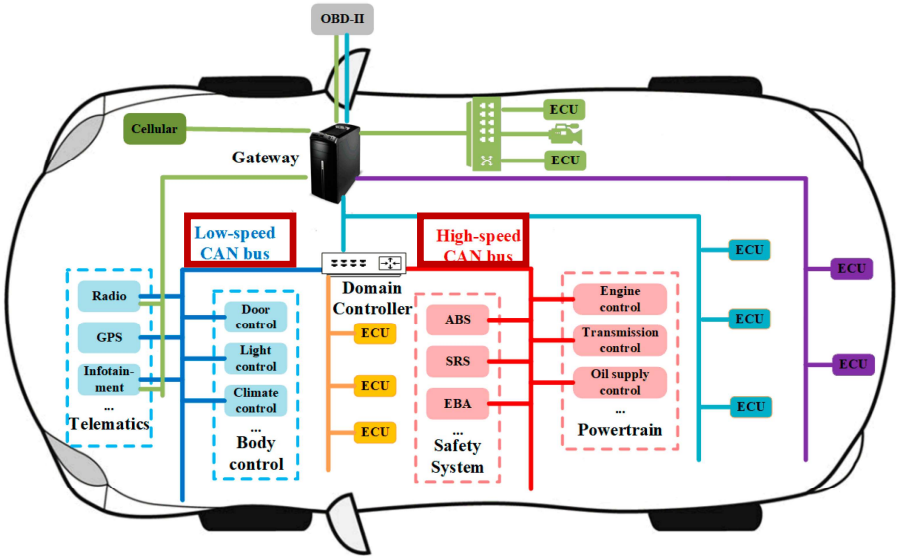
"Perfection is achieved, not when there is nothing more to add, but when there is nothing left to take away." *Antoine de Saint-Exupéry*

http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

LoC=Lines of Code

# Vehicle Networks




GPS: Global Position System
OBD-II: Second On-board Diagnostic

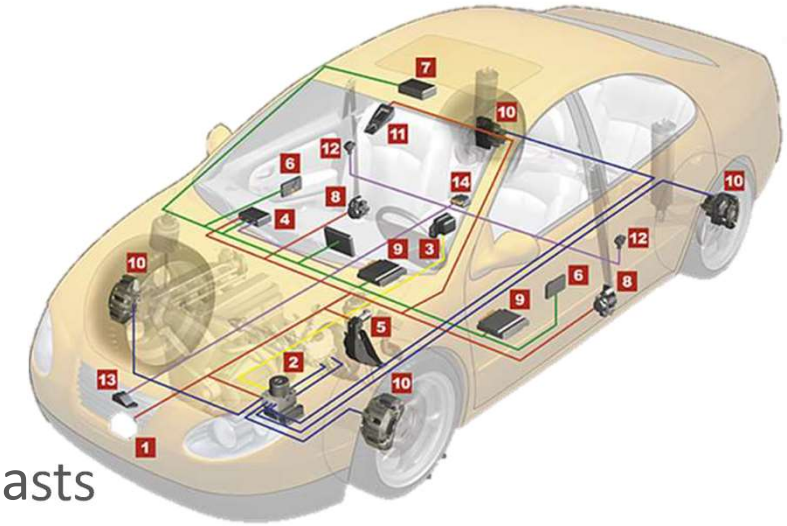
ABS: Anti-skid Brake System
SRS: Supplemental Restraint System
EBA: Emergency Brake Assist

Ethernet
FlexRay
CAN
CAN-High
LIN
CAN-Low

# Entry Points for Hackers

## External

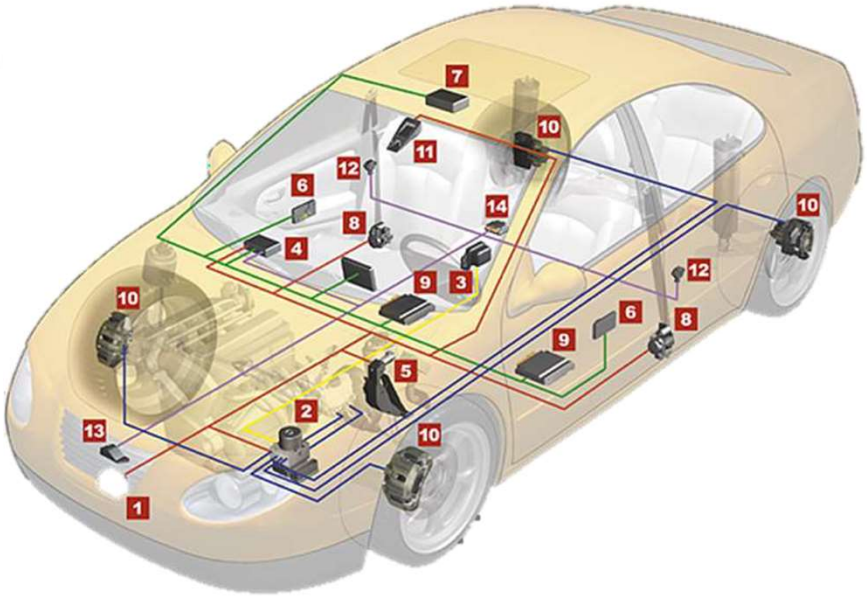
- Bluetooth
- Internet
- Wi-Fi
- Key fob
- LIDAR
- Digital broadcasts
- Tire Pressure Monitors
- Taillight
- DSRC



## Internal

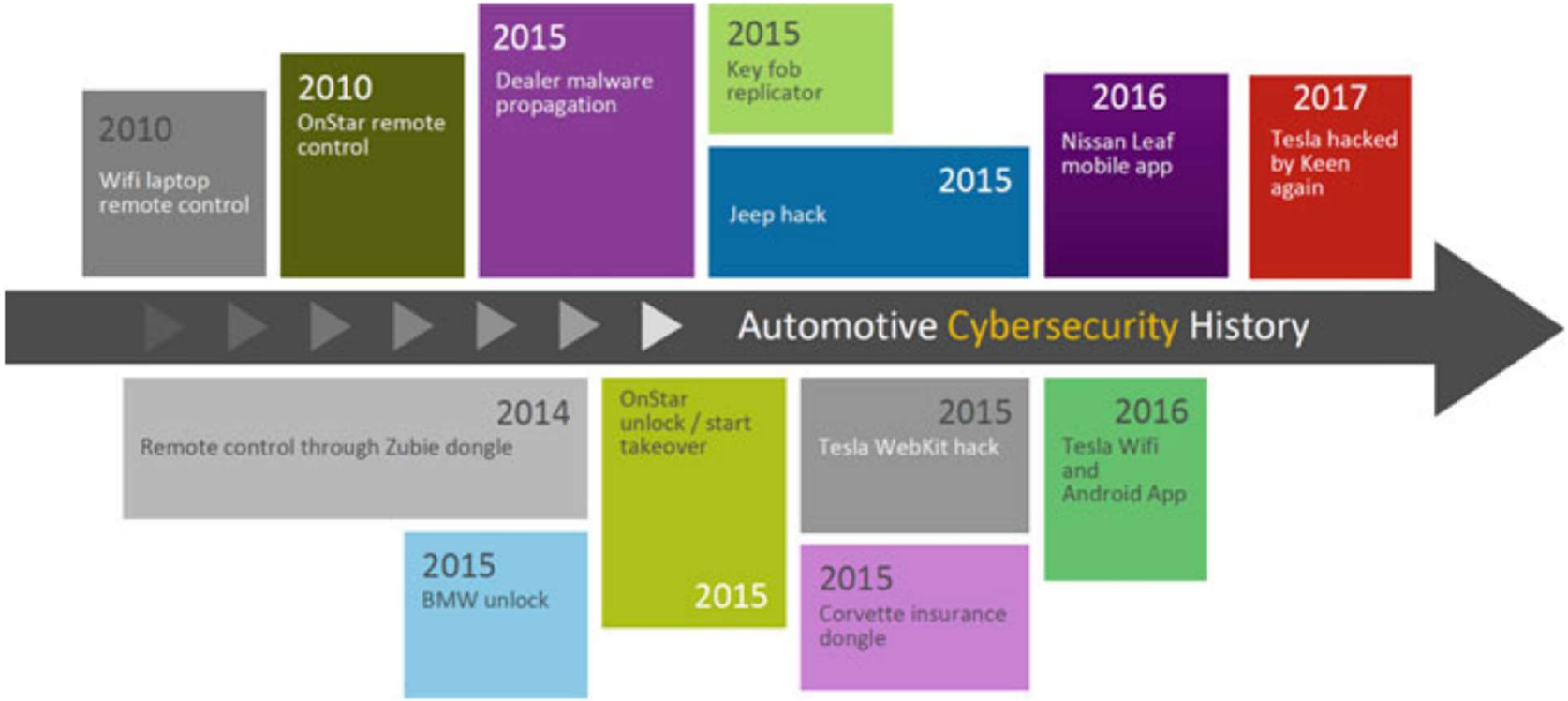
- Diagnostic Port (OBD)
- CD/DVD
- Auxiliary Input Devices (USB)
- CAN Bus
- Auto Ethernet
- Cellular
- Mobile Device Paring

# What Could Go Wrong?



- Theft
- Terrorism
- Revenge
- Mischief
- Extortion – Ransomware
- Insurance fraud
- Espionage
- Stalking
- Feature (de)activation
- Identity theft
- Counterfeiting

# Automotive Security Events



# Vehicle Hacks in Action…

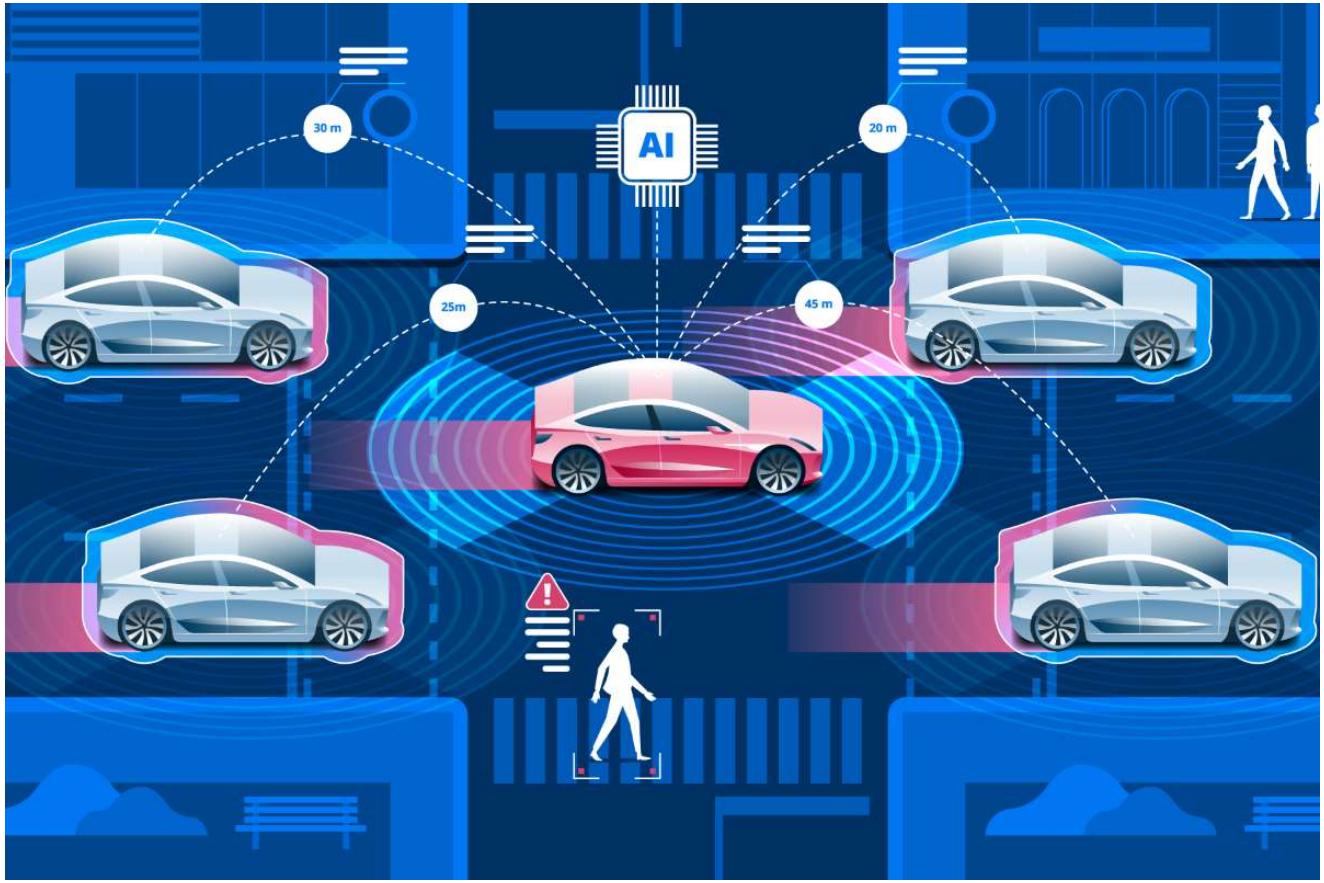
# 2015 Miller & Valasek


Wired, (2015), Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway -- with Me in It'

# The Relay Attack

CNN & West Midland Police Department (UK), (2019), “Relay Attack in Progress”

# Autonomous Vehicles vs. Connected Vehicle



EESI
Environmental and Energy Study Institute

# THE ROAD TO FULL AUTOMATION

## HISTORY OF AUTONOMOUS VEHICLES (AV) IN THE U.S.

**1958**
First car with cruise control is introduced

**1995**
Carnegie Mellon University Navlab project completes cross-country trip with "semi-autonomous" vehicle

**2004**
DARPA Challenges are created to incentivize American autonomous vehicle development

**2009**
Google begins Self-Driving Car Project

**2014**
Google creates first AV prototype

**2015**
Tesla introduces autopilot software; University of Michigan's MCity AV Lab is launched

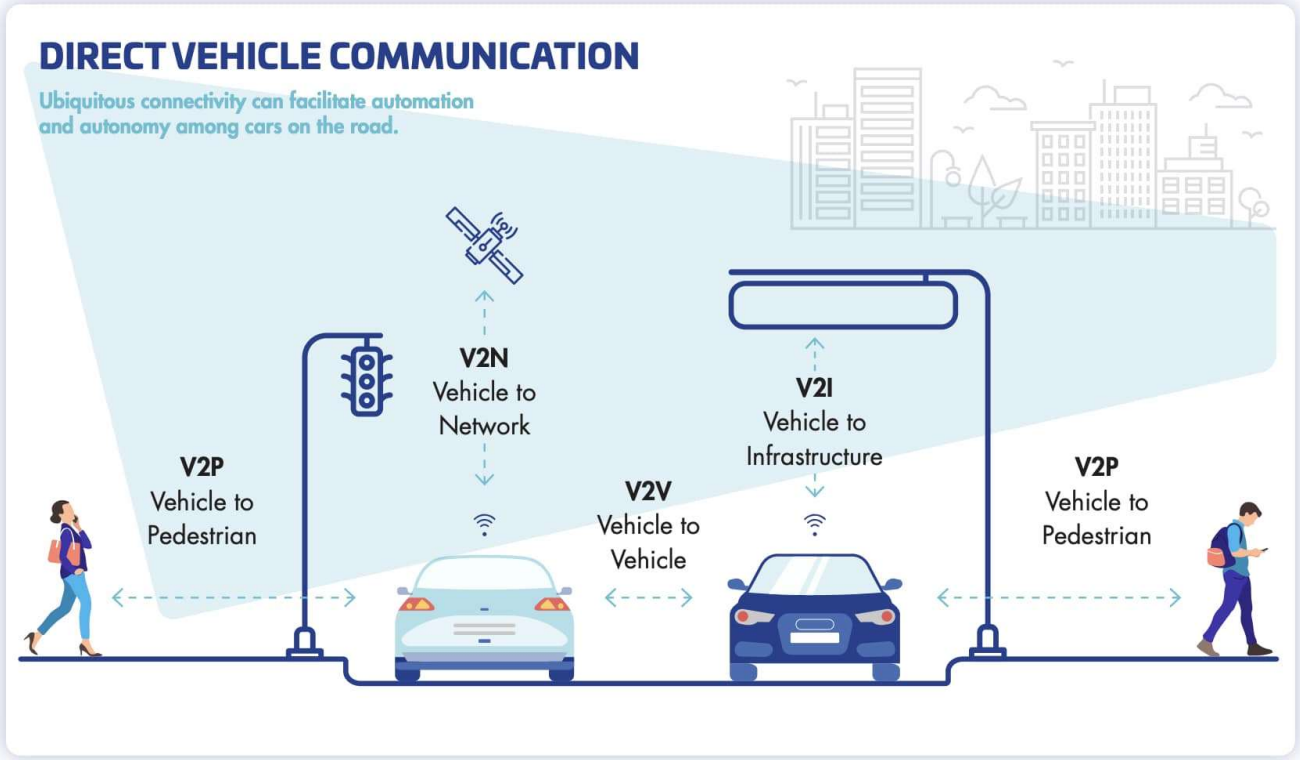
**2016**
First known fatal accident involving a Tesla in autopilot mode. Other accidents followed.

**2018-20**
AV mass transit programs debut in numerous states; NHTSA releases new AV guidance

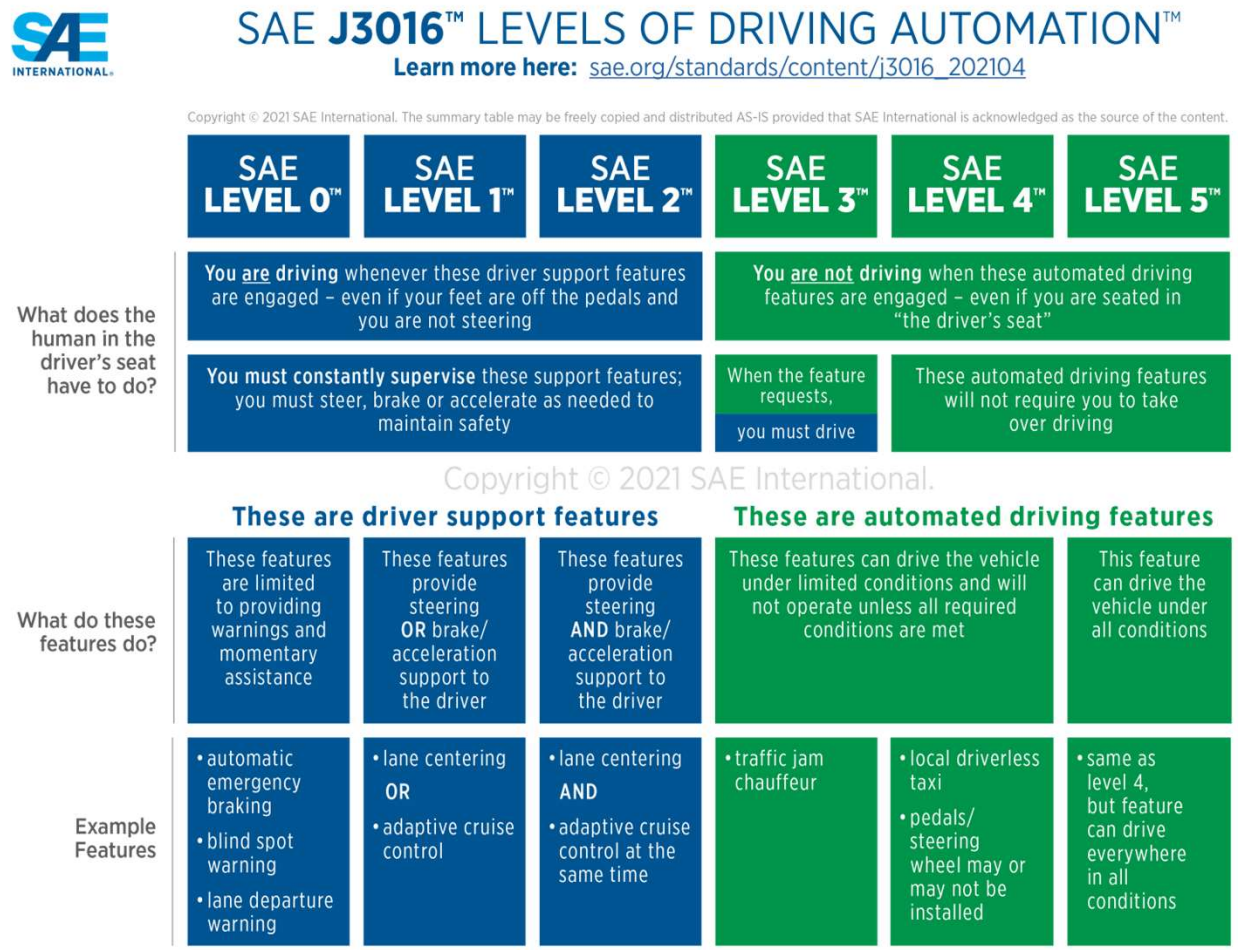
**2021**
Ford and GM invest billions of dollars in AV technology and testing

Graphic by: Sydney O'Shaughnessy
Source: Wikipedia, Reuters, The Verge

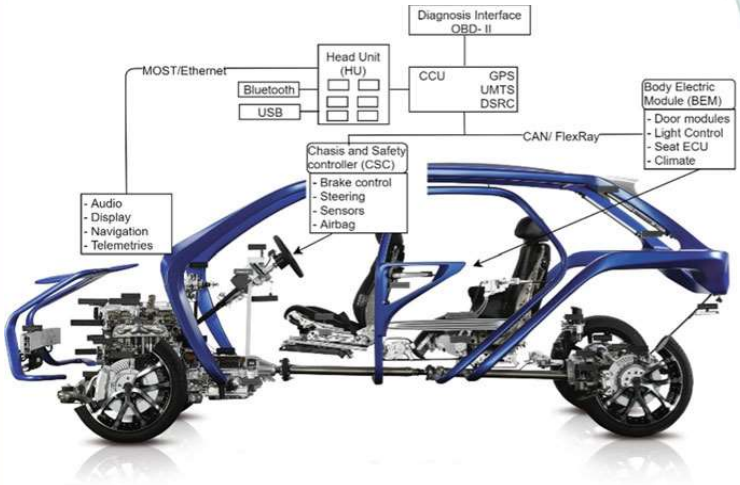
# V2X Communication

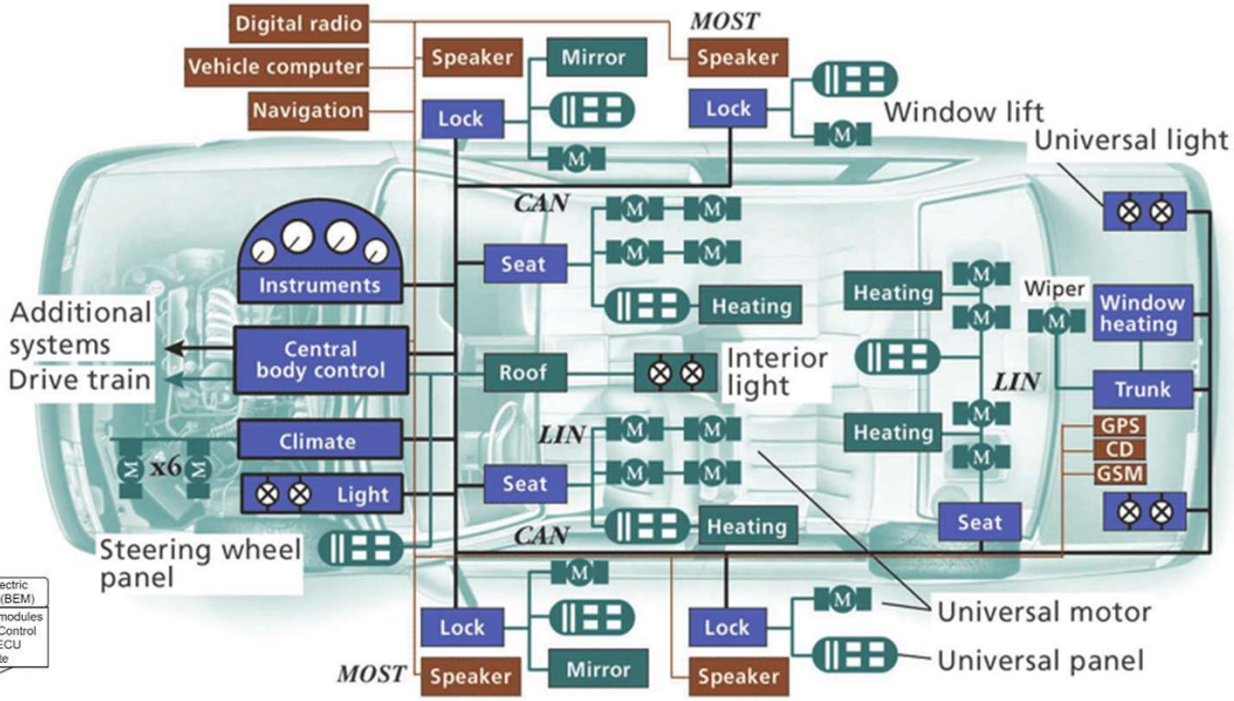


# AV Classification Levels



# Vehicle Connectivity



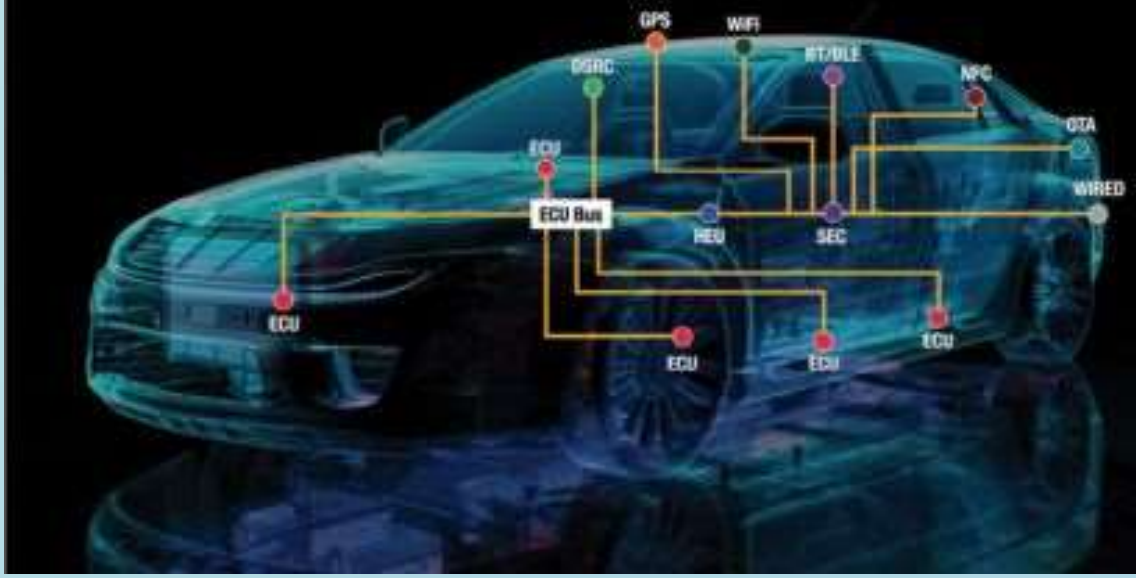




CAN Controller area network
GPS Global Positioning System
GSM Global System for Mobile Communications
LIN Local interconnect network
MOST Media-oriented systems transport

# Need for Cybersecurity in Vehicles

**WIRED**

- OBD-II Port
- Network harness connectors
- Diagnostic ports
- USB ports
- Onboard vehicle networks (CAN, LIN, FlexRay, Ethernet, MOST, etc)
- CD / DVD player
- Vehicle charging port




## Attack surfaces

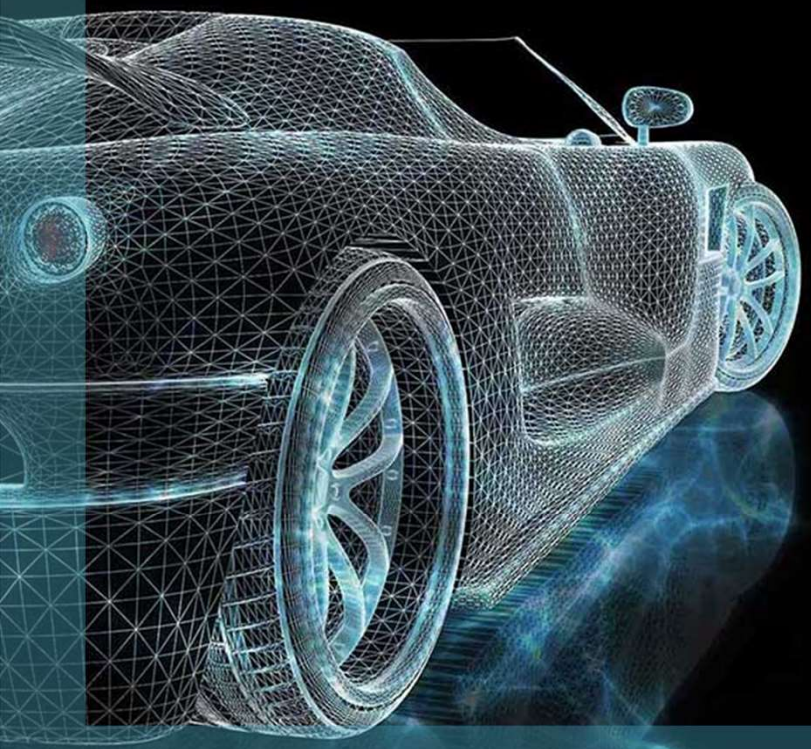
- **ECU** Electronic control unit
- **BT/BLE** Bluetooth / Bluetooth low energy
- **DSRC** Dedicated short range communication
- **GPS** GPS receiver
- **HEU** Head end unit to which ECU bus connects
- **NFC** Near field communication
- **OTA** Over-the-air in-car 4G/LTE connectivity
- **SEC** Vehicle security module
- **WiFi** WiFi

# Vehicle Cyber Engineering (VCE) Graduate Programs

UNIVERSITY OF
DETROIT MERCY
COLLEGE OF ENGINEERING & SCIENCE

# Graduate Certificate - Vehicle Cyber Engineering

This is a 15-credit (five-course) Graduate Certificate Program.

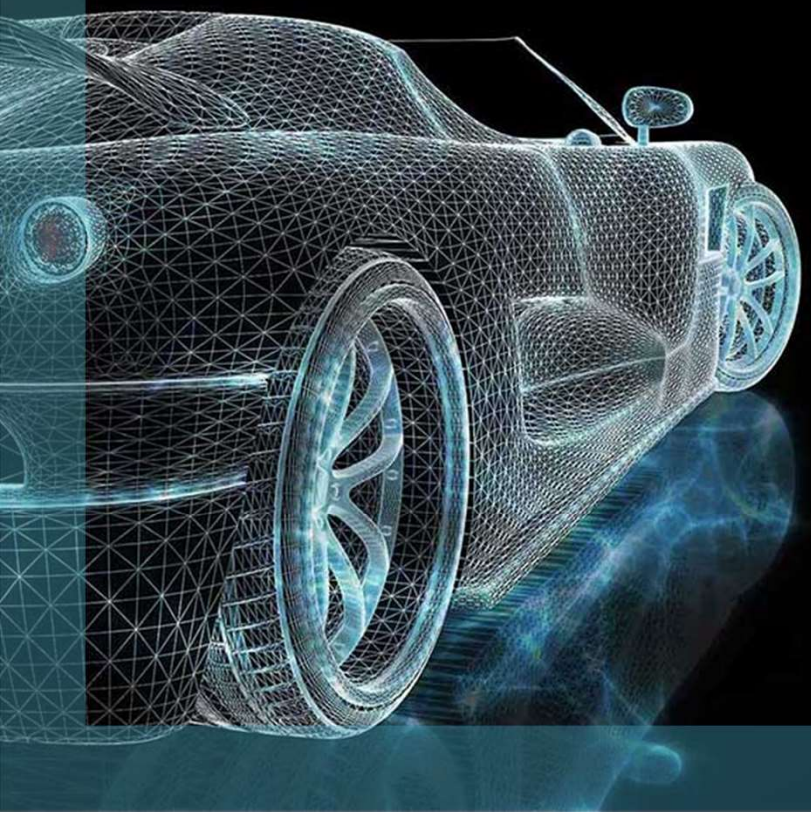


**Required Courses:**

1. CSSE 5545 Advanced Computer Security (3 credits)
2. CSSE 5760 Network Security (3 credits)
3. VCE 5110 Introduction to Cybersecurity (3 credits)
4. VCE 5400 Secure Vehicle Embedded Systems (3 credits)
5. VCE 5500 Secure Vehicle Electronics or
   ELEE 5500 Automotive Electronics (3 credits)

# Master of Science - Vehicle Cyber Engineering

This is a 30-credit (ten-course) Graduate Certificate Program.



**Required Courses (5 Graduate VCE Certificate Courses plus):**

6. VCE 5330 Vehicle Hardware Security (3 credits)
7. ELEE 5150 Secure Wireless Vehicular Networks (3 credits)
8. CSSE 5120 Introduction to Data Science (3 credits) or
   ELEE 5750 Deep Learning (3 credits)
9. ELEE 5350 Machine Learning or
   VCE 5350 Applied Machine learning (3 credits)
10. VCE 5600 Capstone Design (3 credits)


Questions