



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

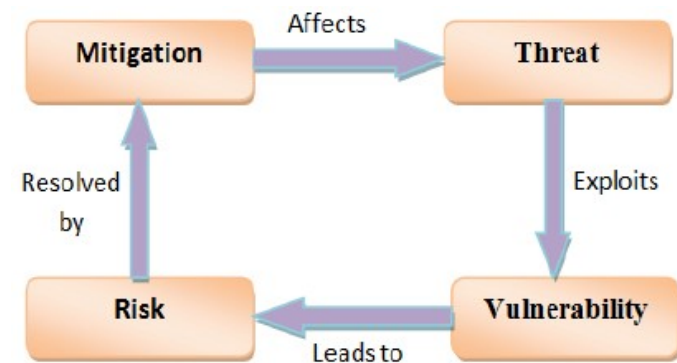
Threat: acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.

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...

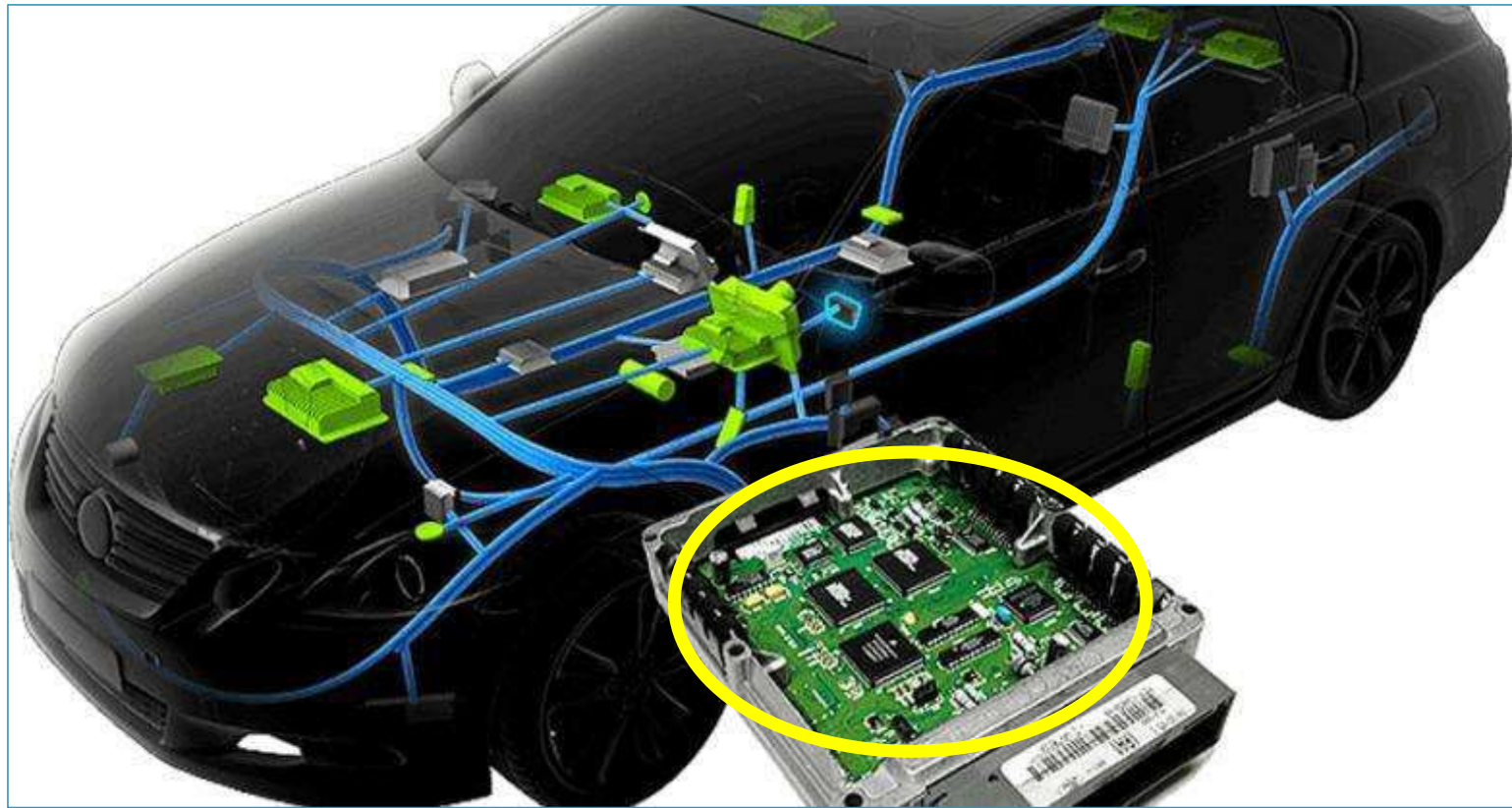
Automotive Cybersecurity

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



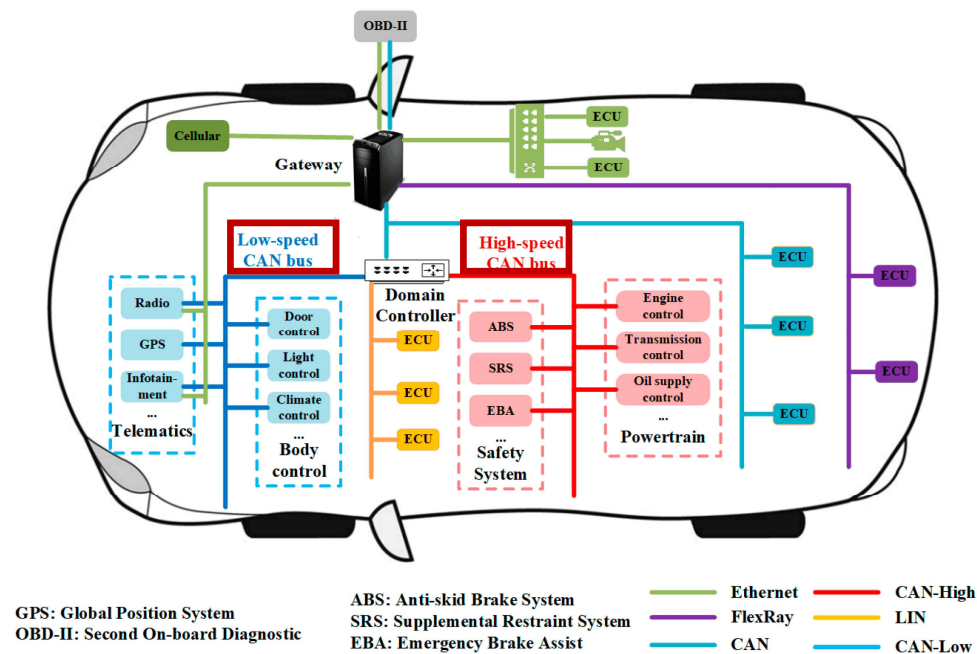
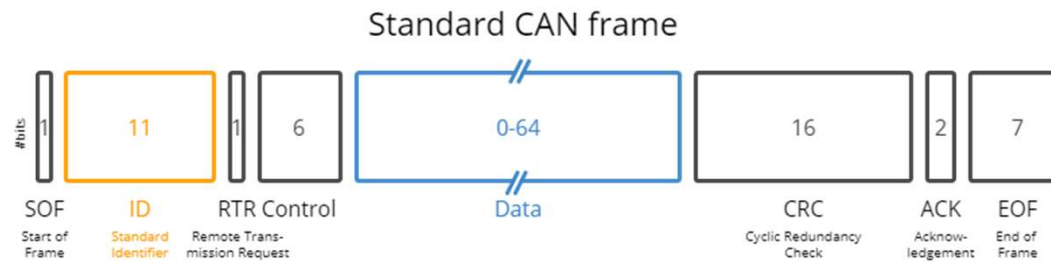
2+ Million LoC

"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

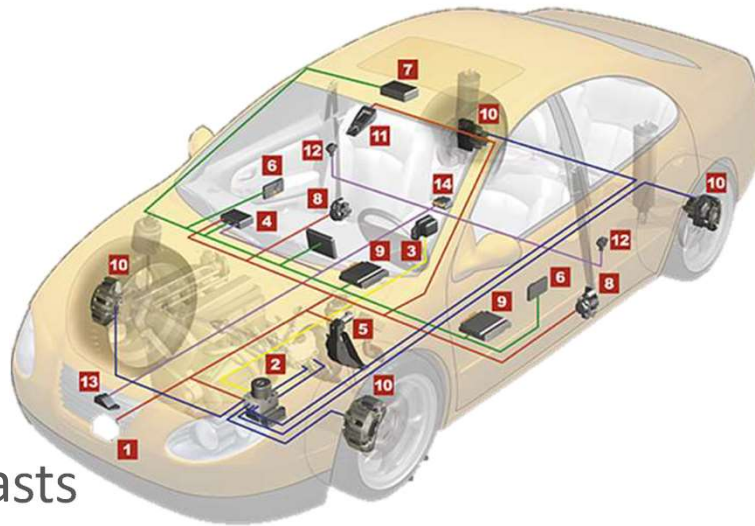
Vehicle Networks



Entry Points for Hackers

External

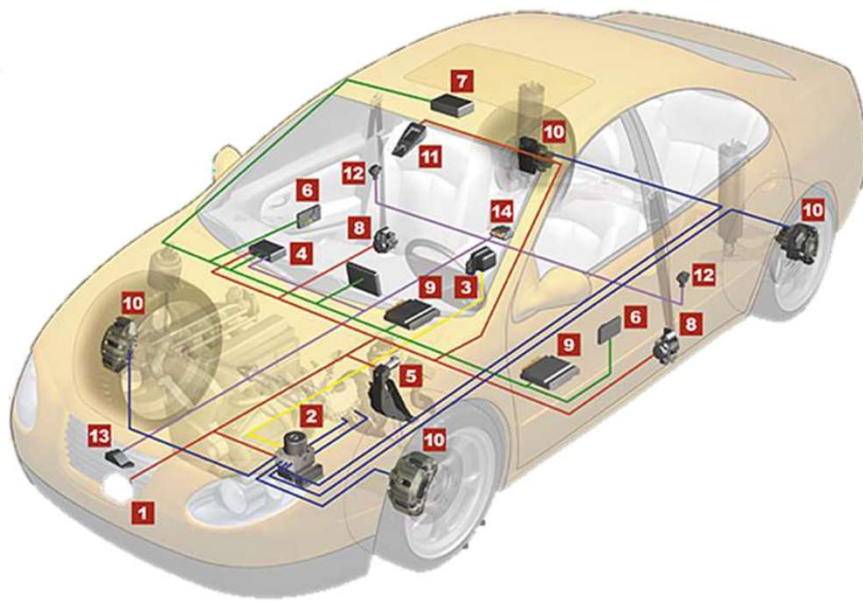
- Bluetooth
- Internet
- Wi-Fi
- Key fob
- LIDAR
- Digital broadcasts
- Tire Pressure Monitors
- Taillight
- DSRC



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

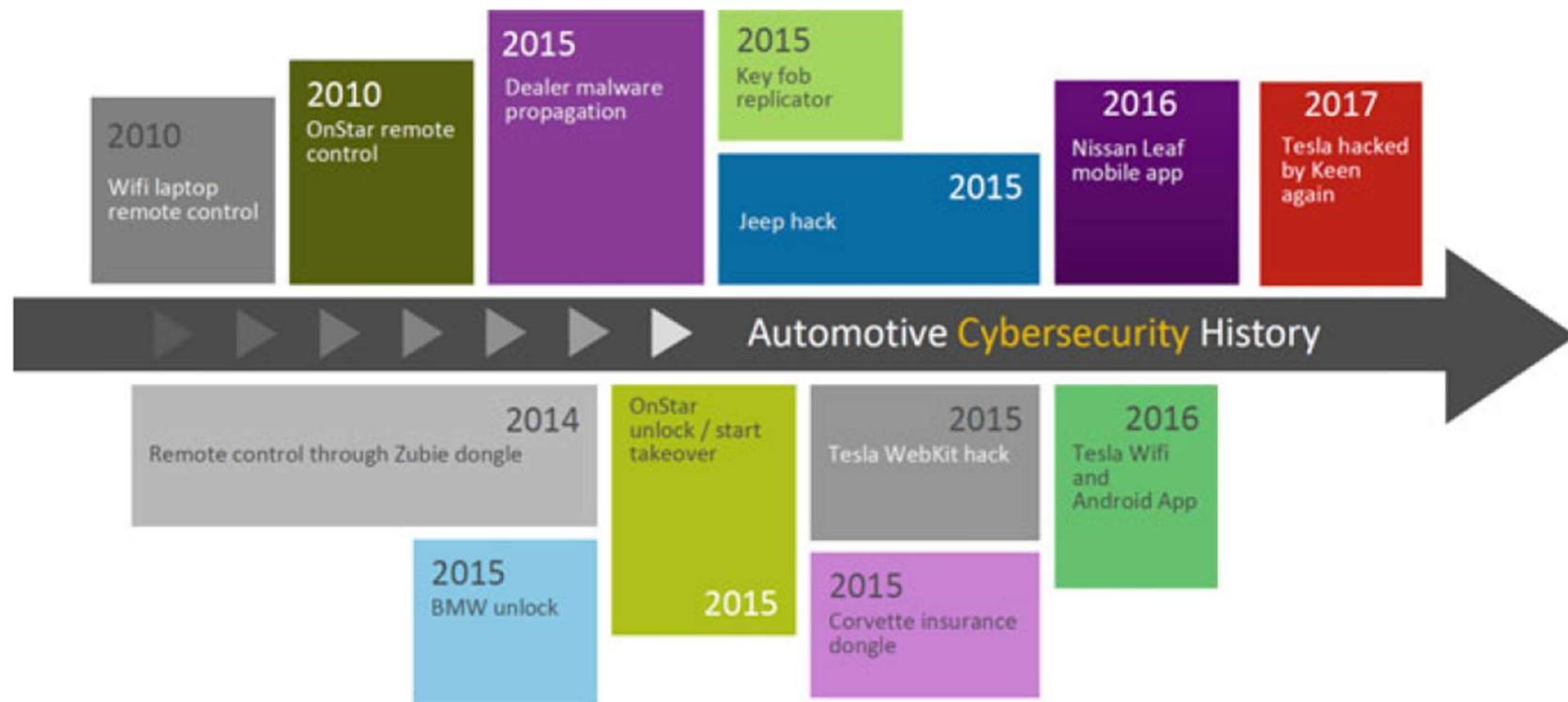
Stalking

Feature
(de)activation

Identity theft

Counterfeiting

Automotive Security Events



Vehicle Hacks in Action...

2015 Miller & Valasek



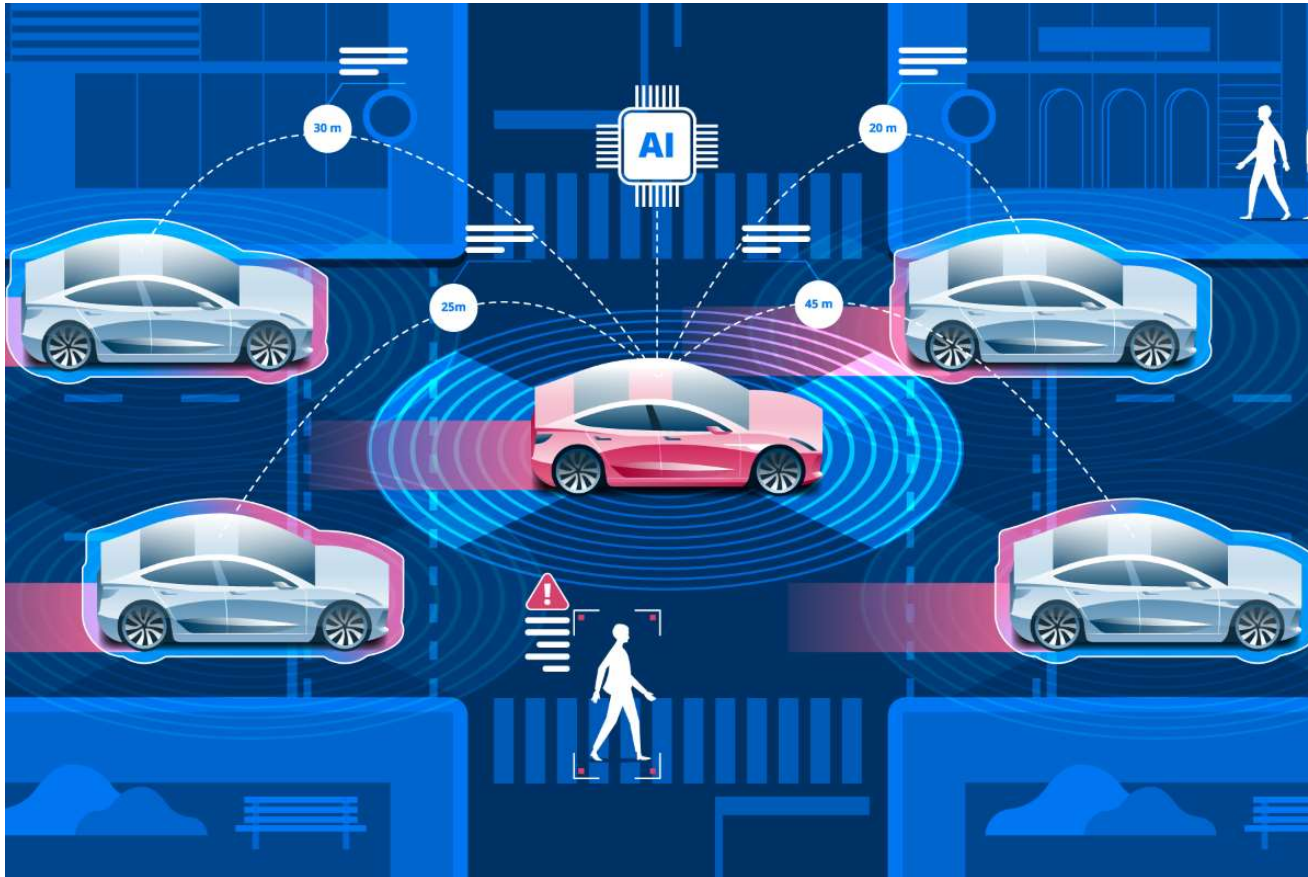
Wired, (2015), Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway -- with Me in It"

The Relay Attack



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

Autonomous Vehicles vs. Connected Vehicle



THE ROAD TO FULL AUTOMATION

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

1958

First car with cruise control is introduced

2004

DARPA Challenges are created to incentivize American autonomous vehicle development

2014

Google creates first AV prototype

2016

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

2021

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

1995

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

2009

Google begins Self-Driving Car Project

2015

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

2018-20

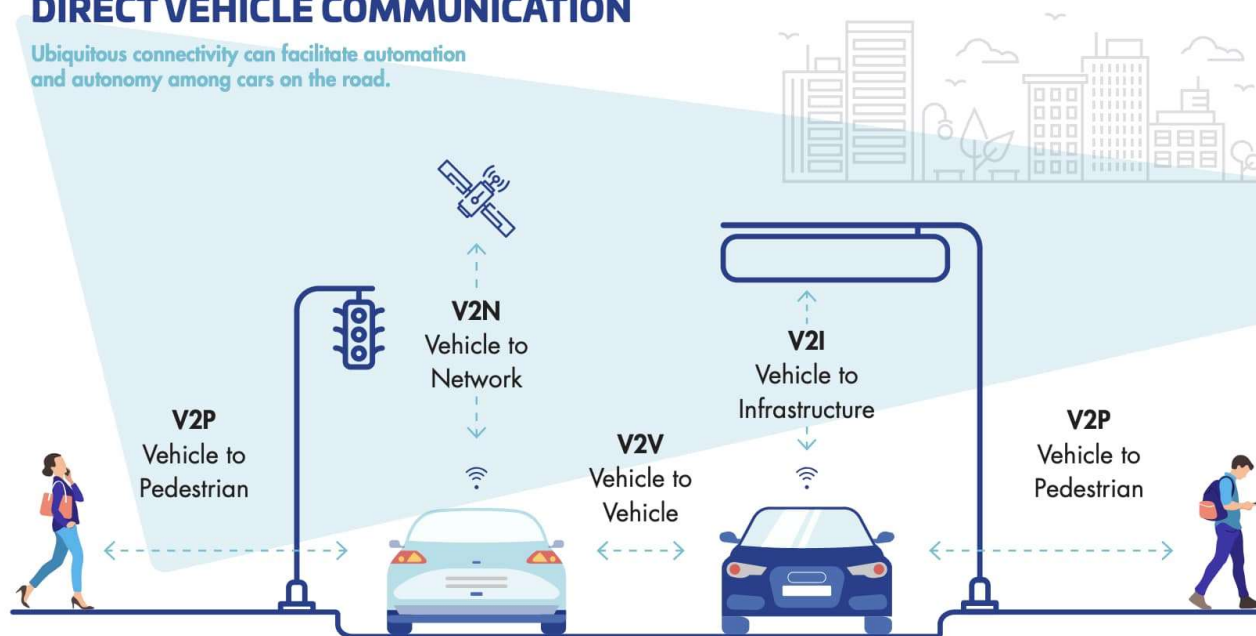
AV mass transit programs debut in numerous states; NHTSA releases new AV guidance

Graphic by: Sydney O'Shaughnessy
Source: [Wikipedia](#), [Reuters](#), [The Verge](#)

V2X Communication

DIRECT VEHICLE COMMUNICATION

Ubiquitous connectivity can facilitate automation and autonomy among cars on the road.



AV Classification Levels



SAE J3016™ LEVELS OF DRIVING AUTOMATION™

Learn more here: [sae.org/standards/content/j3016_202104](https://www.sae.org/standards/content/j3016_202104)

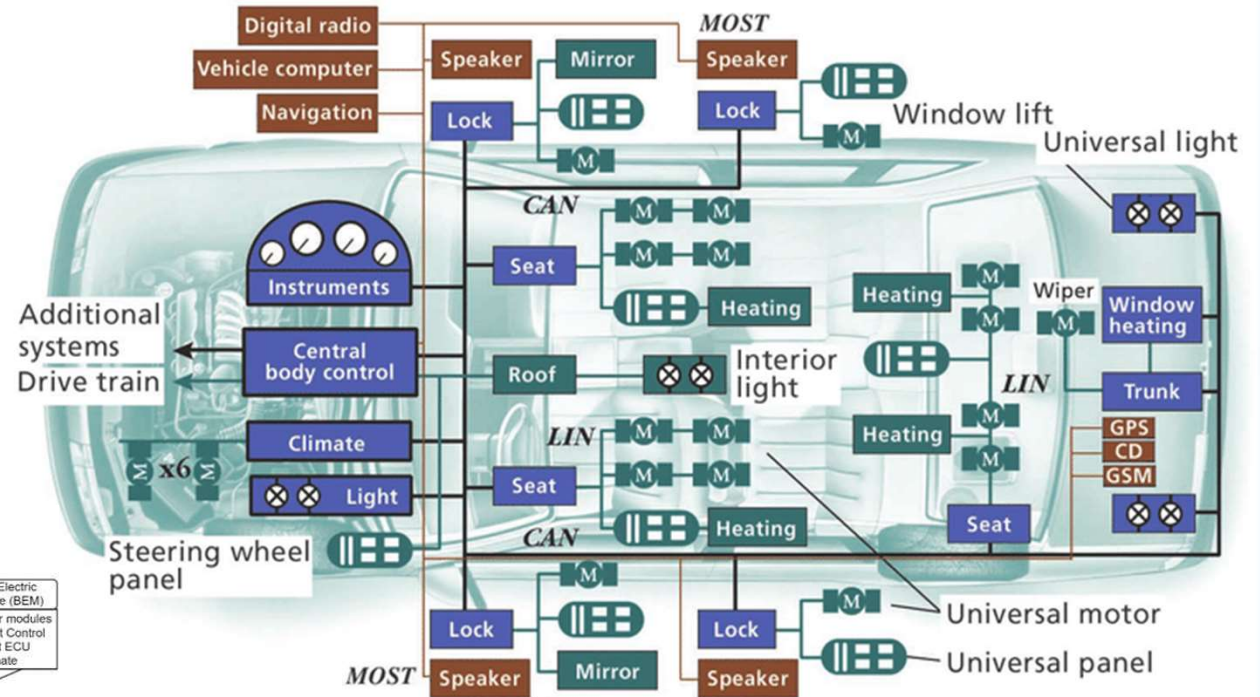
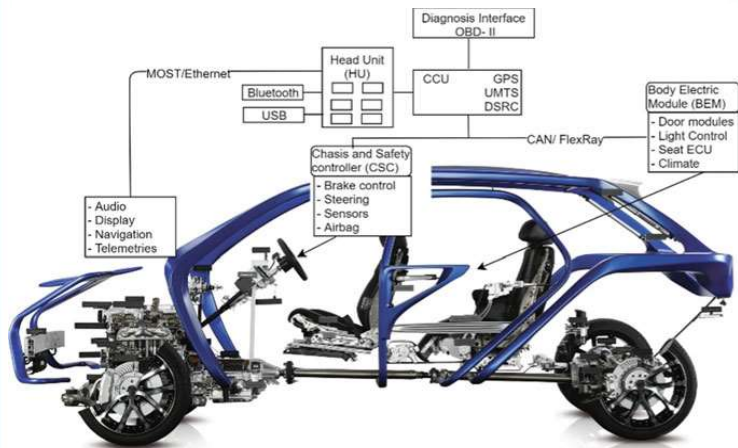
Copyright © 2021 SAE International. The summary table may be freely copied and distributed AS-IS provided that SAE International is acknowledged as the source of the content.

	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
What does the human in the driver's seat have to do?	You <u>are</u> driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You <u>are not</u> driving when these automated driving features are engaged – even if you are seated in “the driver's seat”		
	You <u>must constantly supervise</u> these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	

Copyright © 2021 SAE International.

	These are driver support features			These are automated driving features	
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/acceleration support to the driver	These features provide steering AND brake/acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met	This feature can drive the vehicle under all conditions
Example Features	<ul style="list-style-type: none"> • automatic emergency braking • blind spot warning • lane departure warning 	<ul style="list-style-type: none"> • lane centering OR • adaptive cruise control 	<ul style="list-style-type: none"> • lane centering AND • adaptive cruise control at the same time 	<ul style="list-style-type: none"> • traffic jam chauffeur • local driverless taxi • pedals/steering wheel may or may not be installed 	<ul style="list-style-type: none"> • same as level 4, but feature can drive everywhere in all conditions

Vehicle Connectivity



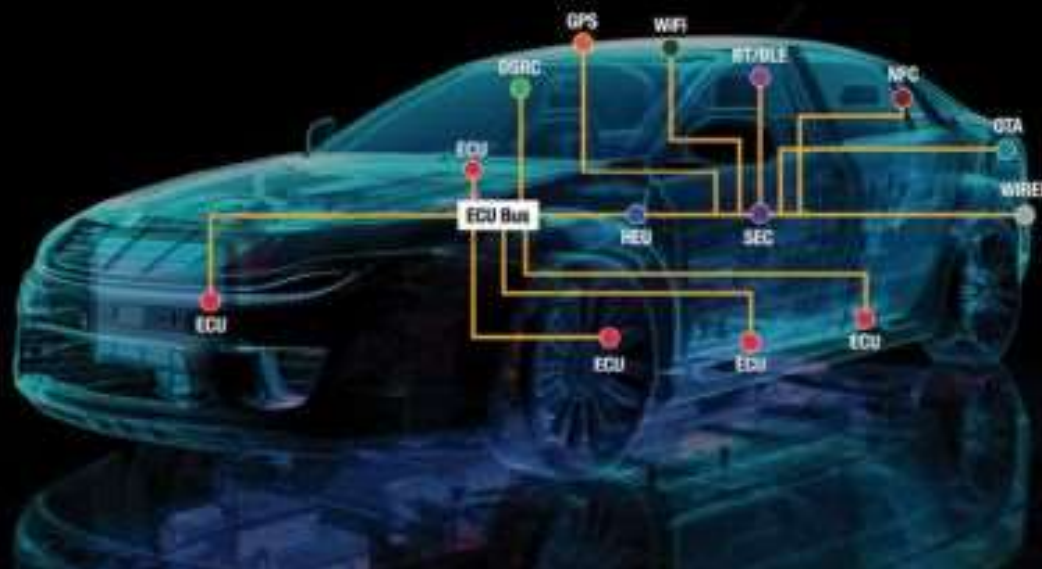
CAN Controller area network
 GPS Global Positioning System
 GSM Global System for Mobile Communications
 LIN Local interconnect network
 MOST Media-oriented systems transport

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

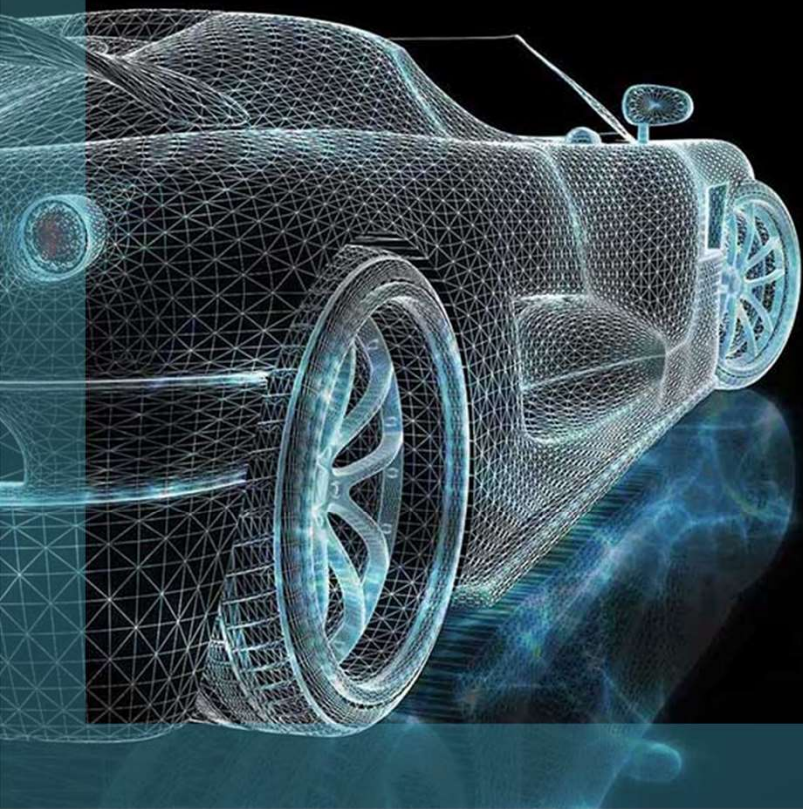


UNIVERSITY OF
DETROIT MERCY

COLLEGE OF ENGINEERING & SCIENCE

Graduate Certificate - Vehicle Cyber Engineering

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



Required Courses:

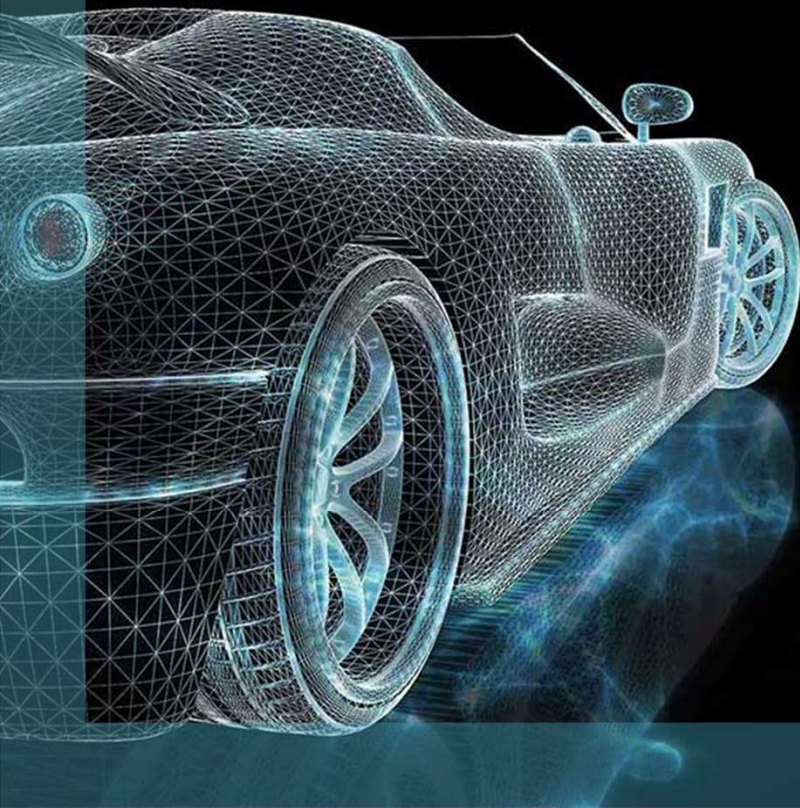
1. CSSE 5545 Advanced Computer Security (3 credits)
2. CSSE 5760 Network Security (3 credits)
3. VCE 5110 Introduction to Cybersecurity (3 credits)
4. VCE 5400 Secure Vehicle Embedded Systems (3 credits)
5. VCE 5500 Secure Vehicle Electronics or
ELEE 5500 Automotive Electronics (3 credits)

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)



The background of the slide features a collage of paper cutouts. Several light gray paper heads are arranged in a circular pattern, each with a large black question mark on its face. In the center, a light blue paper head is positioned, featuring a blue line drawing of a lit lightbulb with rays emanating from it. The word "Questions" is written in a white serif font across the center of the slide, partially overlapping the central head and the other heads in the background.

Questions