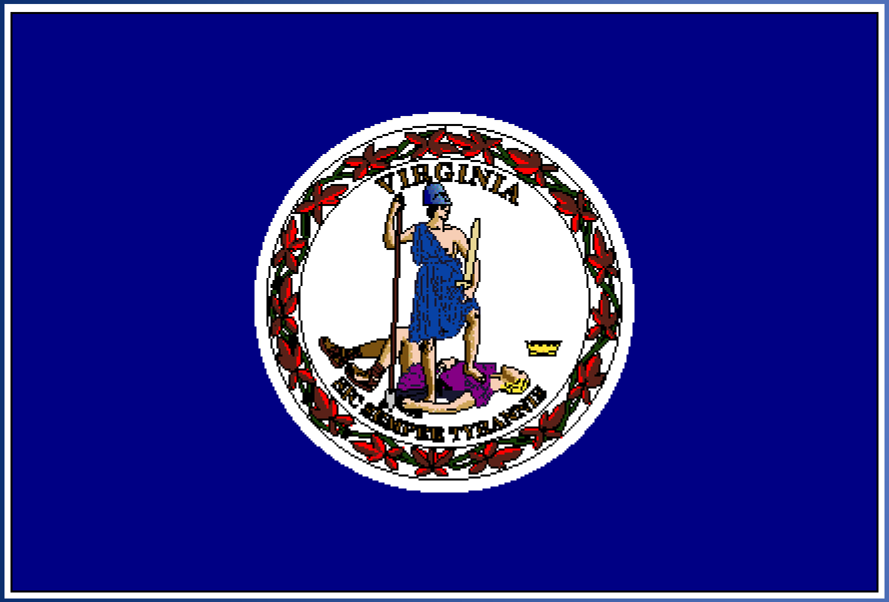
Distracted Driver Summit
September 29, 2017



Captain Jerry L. Davis
Virginia State Police
Bureau of Criminal Investigation – Wytheville Field Office

Autonomous Vehicles and the Impact on Law Enforcement

What is it?
Autonomous vs Connected technology
Regulation
Liability / Insurance
Cyber concerns
Questions


JOHN CARPENTER'S
CHRISTINE

TRANSPORTATION SYSTEM

250 Million Vehicles

4 Trillion Passenger Miles

1.3 Trillion Motor Carrier Ton Miles

4 Million Miles of Roadway

Supports generation of 15.685 billion in GDP

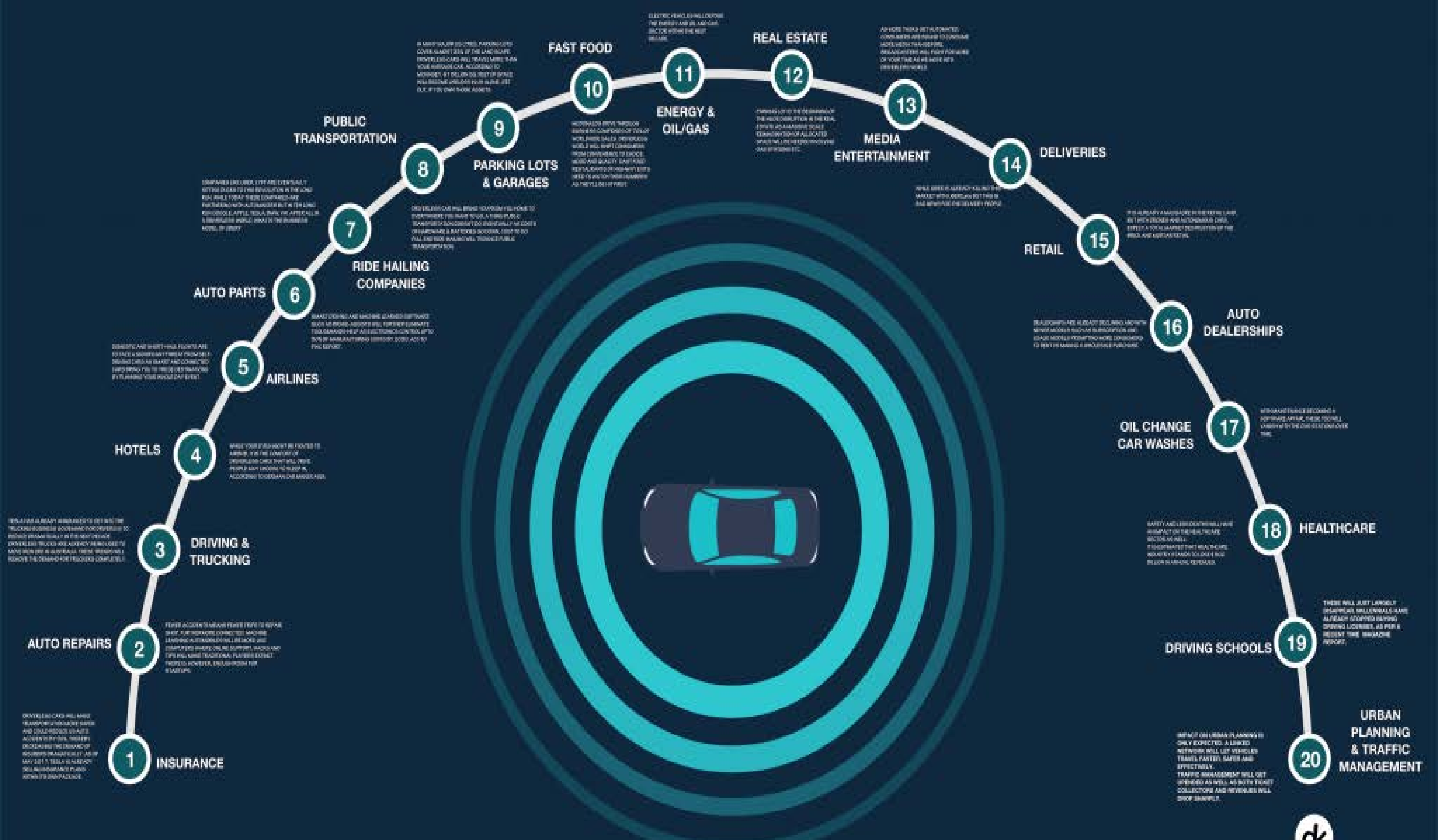
Background Research | Benefits of Autonomous Driving Cars

SAFETY	COST	HEALTH	TIME	ENV
Could save more than **30,000 lives annually**	Insurance costs **reduced** or **eliminated**	Facilitates **personal independence** and mobility for physiologically & mild cognitive limitations.	Less wrecks = less traffic congestion, **saving time**	**Reduction** in heavy safety features, crumple zones, and airbags
Prevents accidents during unanticipated health issues: heart attack, seizure, stroke, etc.	Minimize the risk of **traffic fines**	Reduction in **ER visits, hospitalizations**		Lighter weight; lowers **fuel consumption** and **emissions**
Impaired drivers less of a danger to others				

Eno Center for transportation, (2013). *Preparing the nation for autonomous vehicles: opportunities, barriers and policy recommendations.* Washington, DC.

KPMG and CAR (2012). *Self-Driving Cars: The Next Revolution.* Ann Arbor, MI.

20 INDUSTRIES AUTONOMOUS VEHICLES WILL DISRUPT BY 2025

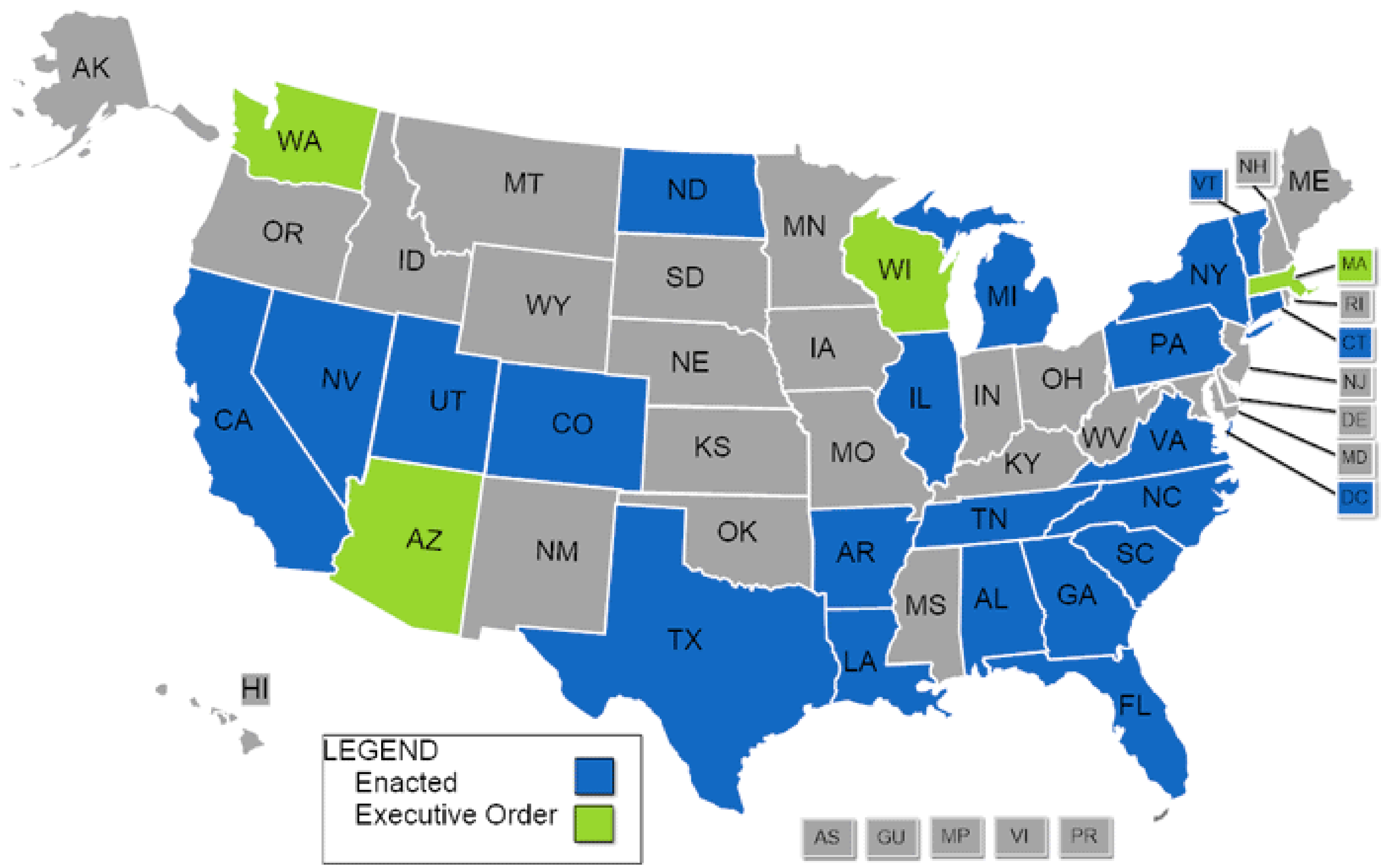


Sources: CB Insights, McKinsey, Google Search, BCG, Economist, WEF, Statista.


Police
M.C.I.U.


Oakland
San Jose
San Francisco
3 RIGHT LANES
Powell Street
Emeryville

Enacted Autonomous Vehicle Measures
Source : National Conference of State Legislators



Great Mileage

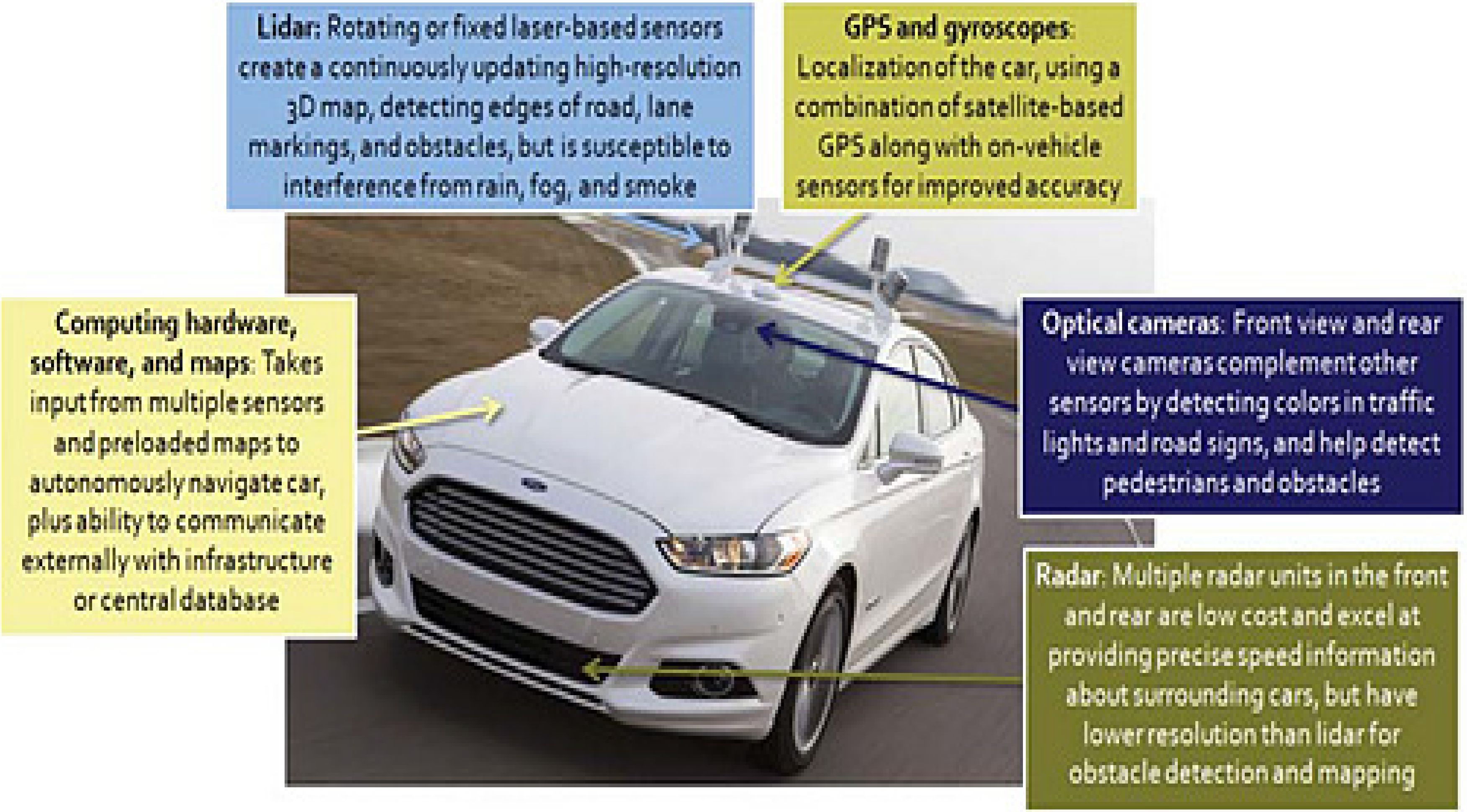
Some Benefits of the Driverless Car

Google's Aspiration	Potential Annual Benefits (US only)
• 90% reduction in accidents	• 4.95 million fewer accidents • 30,000 fewer deaths • 2 million fewer injuries • $400 billion in accident-related cost savings
• 90% reduction wasted commuting	• 4.8 billion fewer commuting hours • 1.9 billion gallons in fuel savings • $101 billion saved in lost productivity and fuel costs
• 90% reduction in cars	• Reduce cost per trip-mile by 80% or more • Increase car utilization from 5-10% to 75% or more • Better land use

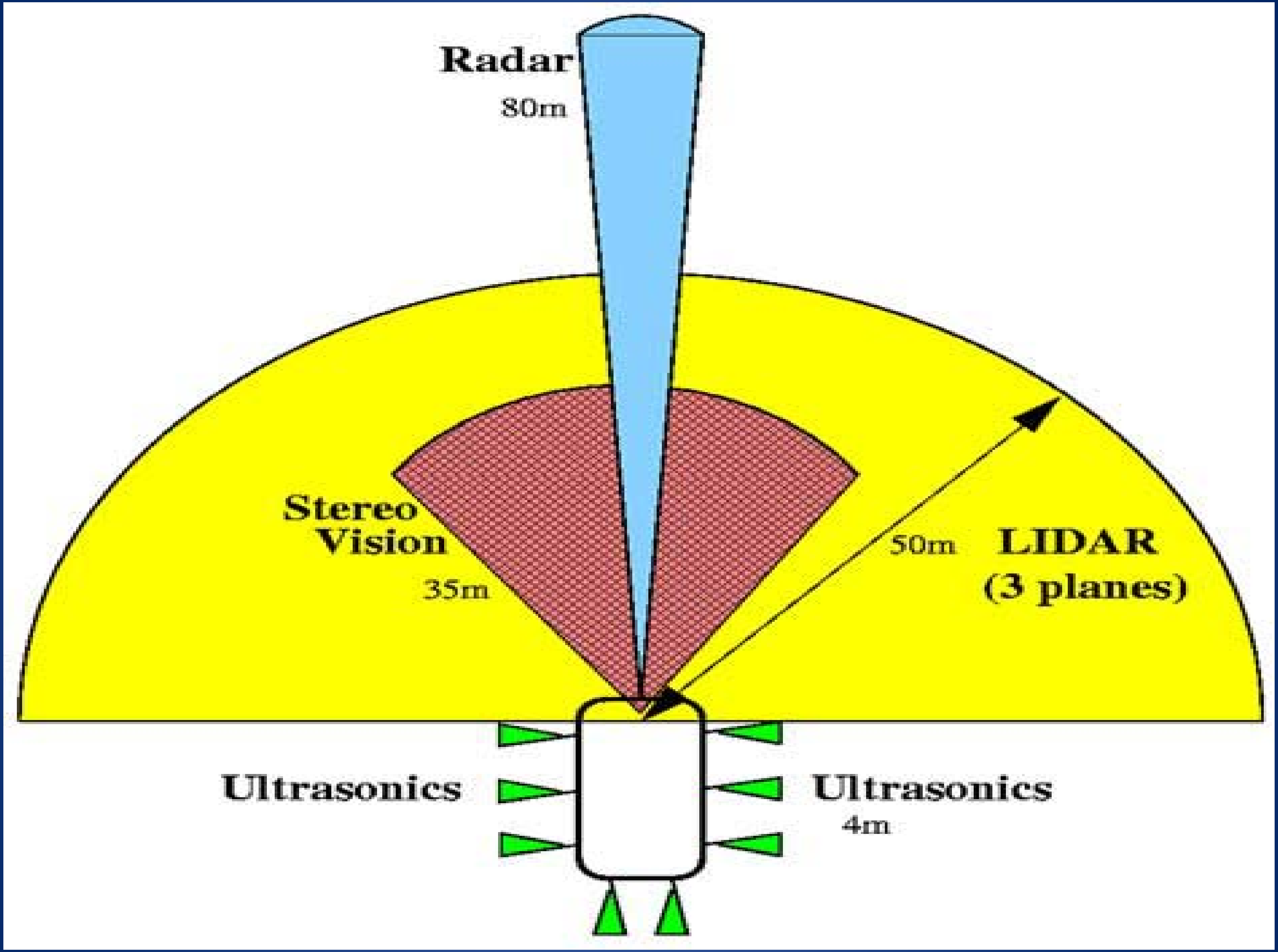
Sources: Google, US NHTSA, AAA, Texas A&M Transportation Institute, Columbia University Earth Institute and Devil's Advocate Group's analysis


Google
self-driving car
HYBRID

A Combination of Sensors Enable Autonomous Vehicle Capabilities



Source: Lux Research, Inc.



Sensing system components and
effective ranges.


AGELAB
1200
66-911S
VirginiaTech
Invent the Future®

LEVELS OF AUTONOMY NHTSA

Level 0	The human driver is in complete control of all functions of the car
Level 1	One function is automated
Level 2	More than one function is automated at the same time, but the driver remains attentive
Level 3	Driving functions are sufficiently automated - the driver can safely engage in other activities
Level 4	The car is self-driving - no human driver required

LEVELS OF AUTONOMY
Society of Automotive Engineers
SAE

Level 0 – **No Automation**: The full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems

Level 1 – **Driver Assistance**: The driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task

Level 2 – **Partial Automation**: The driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task

Level 3 – **Conditional Automation**: The driving mode-specific performance by an Automated Driving System of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene

Level 4 – **High Automation**: The driving mode-specific performance by an Automated Driving System of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene

Level 5 – **Full Automation**: The full-time performance by an Automated Driving System of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver

PLATOONING


Driver??


NHTSA rules that AI can be sole driver of Google's self-driving cars Highway Administration ruling means steering wheel, pedals not needed.

Sebastian Anthony (UK) - 2/10/2016, 8:46 AM : ARS Technica


INSURANCE
FRAUD


KIDNAPPING


DRUGS


© PA

>2025
FULLY AUTOMATED
2020
HIGHLY AUTOMATED
2016
PARTIALLY AUTOMATED

Federal Automated Vehicles Policy

Accelerating the Next Revolution In Roadway Safety

September 2016

This Policy is an important early step in that effort. We are issuing this Policy as agency guidance rather than in a rulemaking in order to speed the delivery of an initial regulatory framework and best practices to guide manufacturers and other entities in the safe design, development, testing, and deployment of HAVs. In the following pages, we divide the task of facilitating the safe introduction and deployment of HAVs into four sections:

Vehicle Performance Guidance for Automated Vehicles

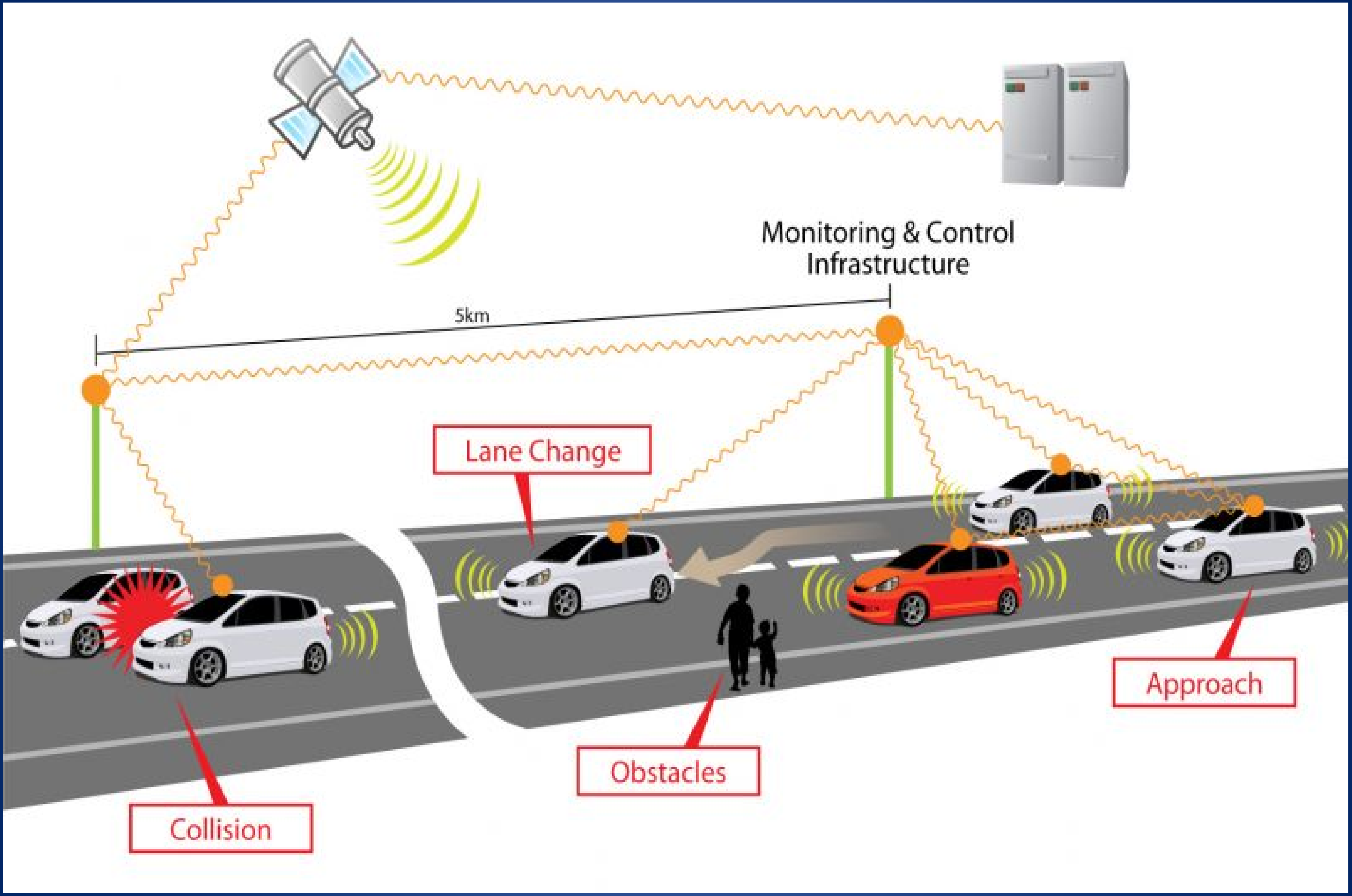
Model State Policy

NHTSA's Current Regulatory Tools

New Tools and Authorities

Connected Vehicle Environment

Connected Vehicle Concept (U.S. Department of Transportation)

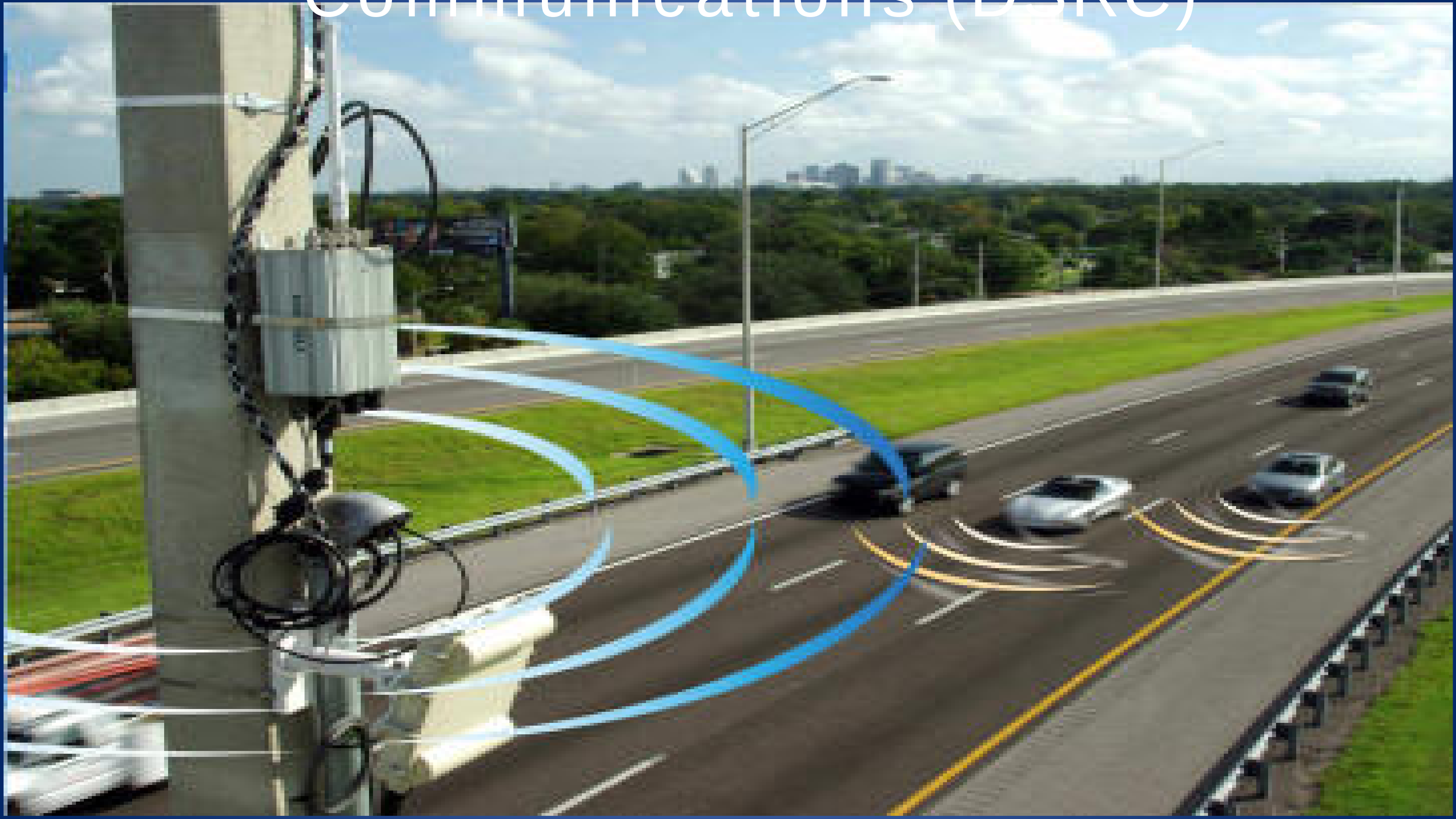

Monitoring & Control
Infrastructure
5km
Lane Change
Approach
Obstacles
Collision

Vehicle to Mobile Devices

Android Auto App

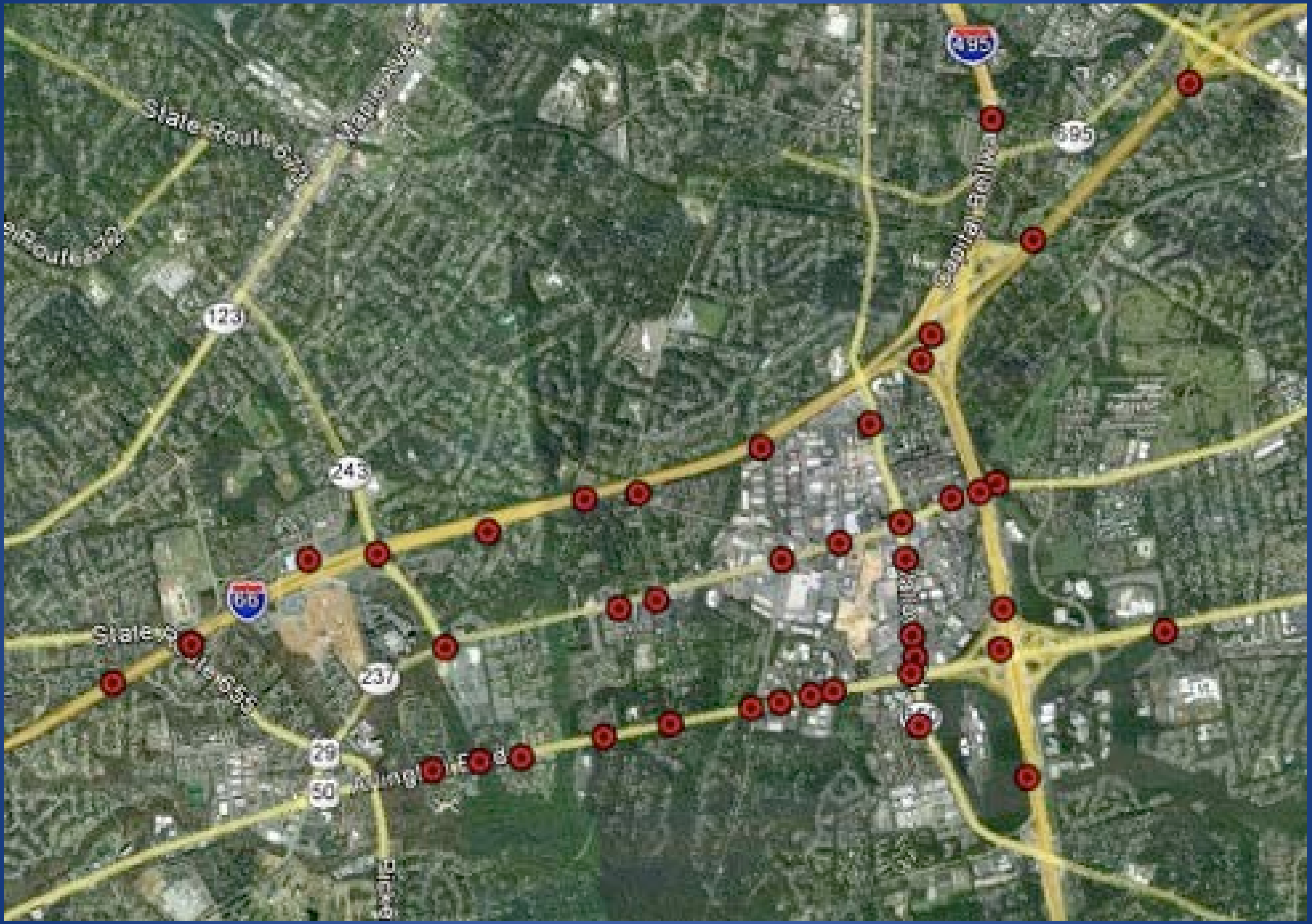
Apple CarPlay App

Dedicated Short Range Communications (DSRC)



http://www.dailywireless.org/2011/10/14/world-congress-on-talking-cars/

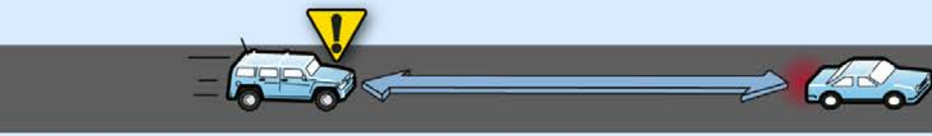
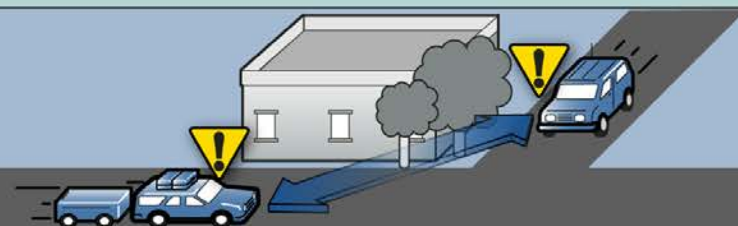
Interstate 66 VDOT Connected Road Test Bed: Fairfax County



VDOT Virginia Department of Transportation

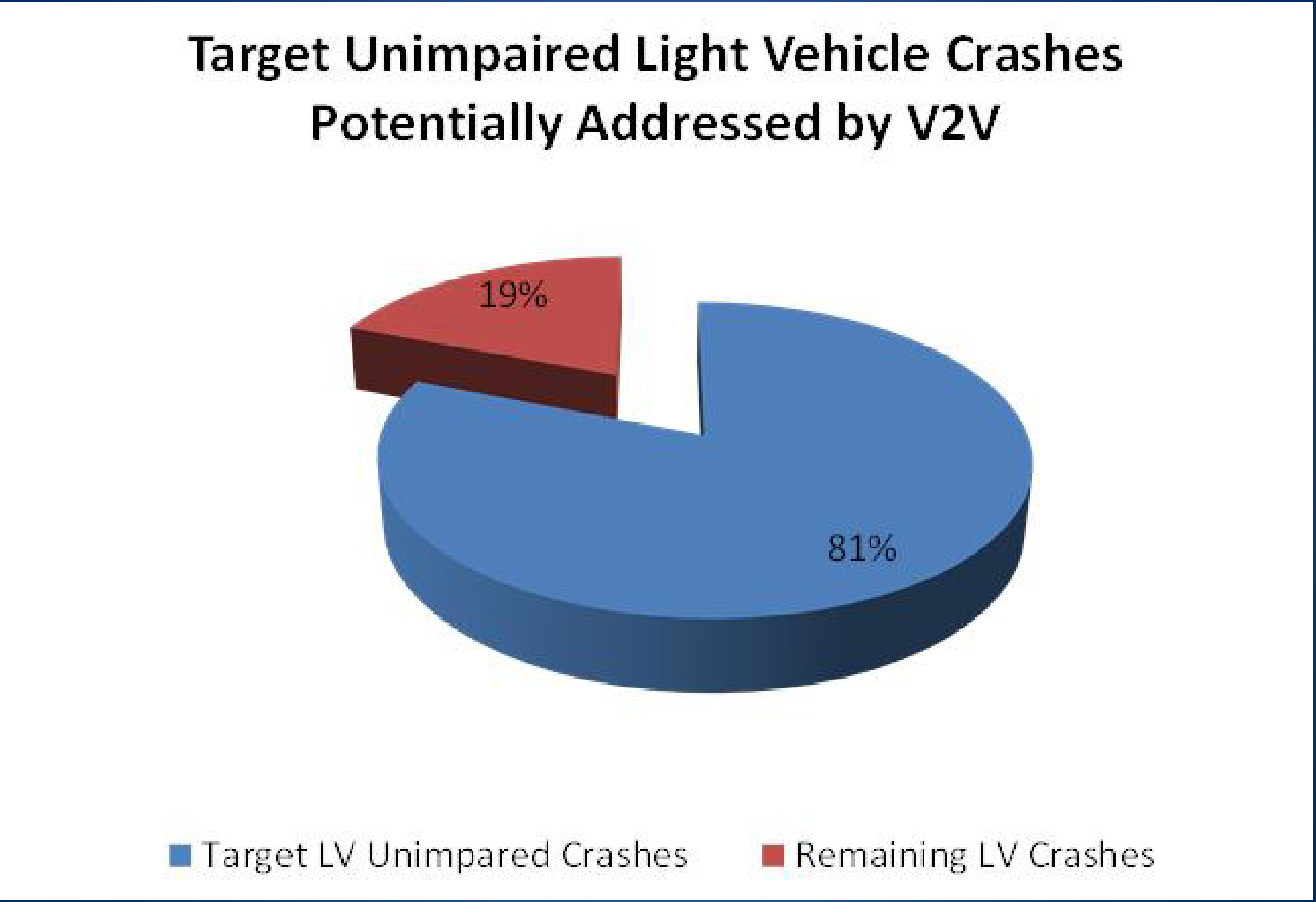
VTRC Virginia Transportation Research Council

Virginia Tech Transportation Institute

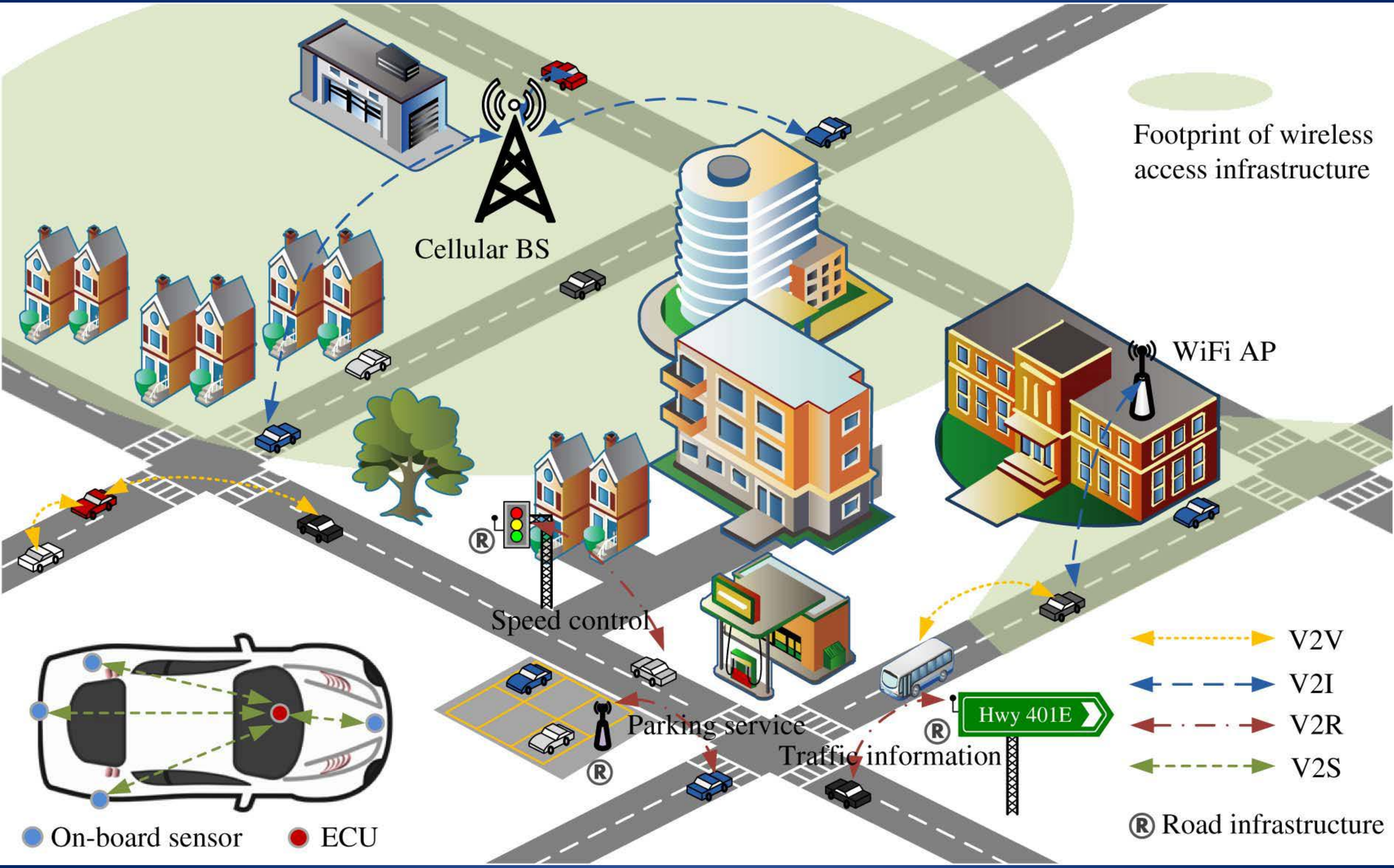
Scenario and warning type		Scenario example
Rear end collision scenarios	**Forward collision warning** Approaching a vehicle that is decelerating or stopped.	
	Emergency electronic brake light warning Approaching a vehicle braking hard or stopped in roadway but not visible due to obstructions.	
Lane change scenarios	**Blind spot warning** Beginning lane change that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles already in or soon to be in blind spot.	
	Do not pass warning Encroaching onto the travel lane of another vehicle traveling in opposite direction.	
Intersection scenario	**Intersection warning** Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.	

To view a video demonstration of selected V2V safety applications, go to...
http://www.gao.gov/products/GAO-14-13

Source: GAO analysis of Crash Avoidance Metrics Partnership information.



Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application


Footprint of wireless access infrastructure
Cellular BS
WiFi AP
Speed control
Parking service
Traffic information
Hwy 401E
V2V
V2I
V2R
V2S
Road infrastructure
On-board sensor
ECU

Basic Safety Message

Transmitted every tenth of a second and contains:

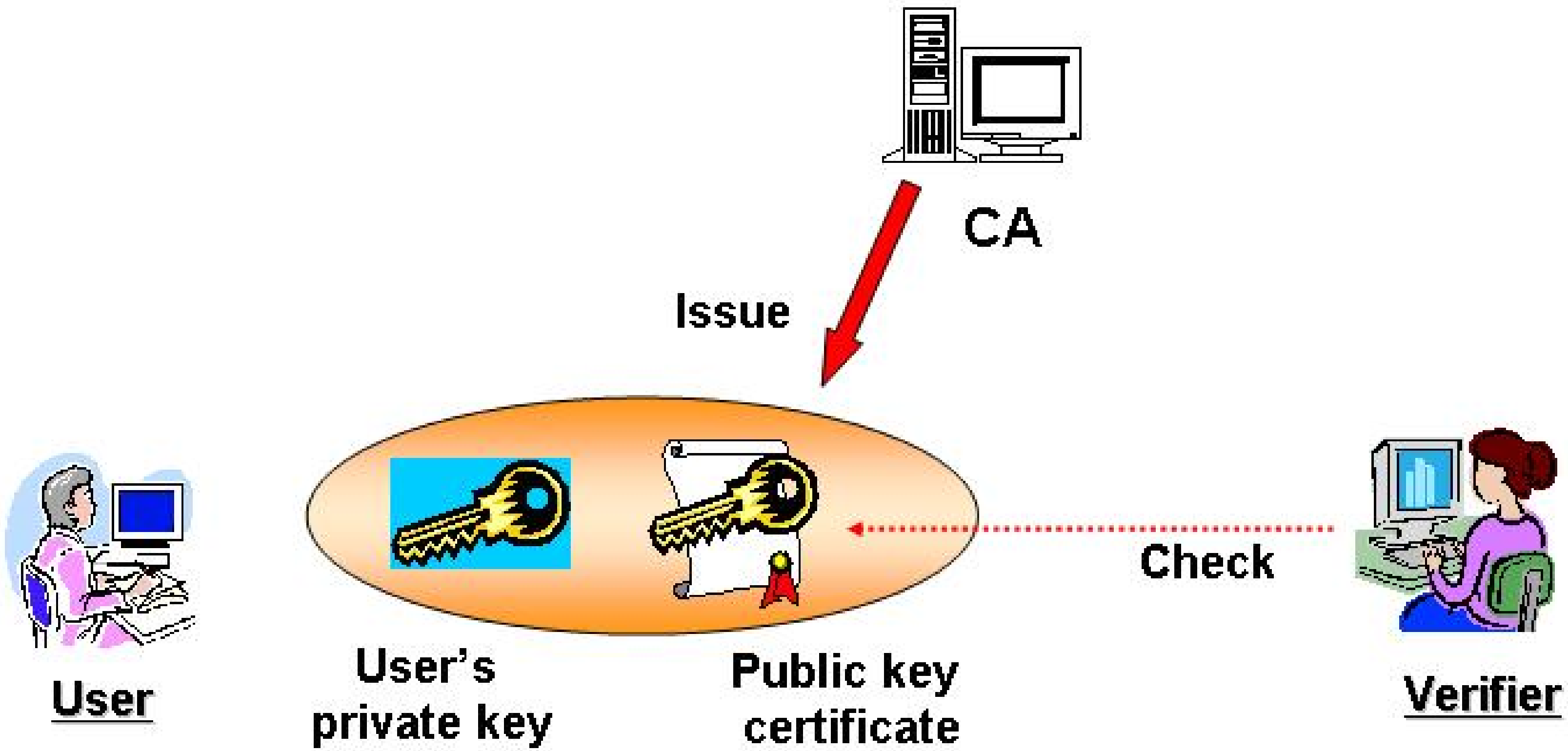
GPS Position
Speed
Acceleration
Heading

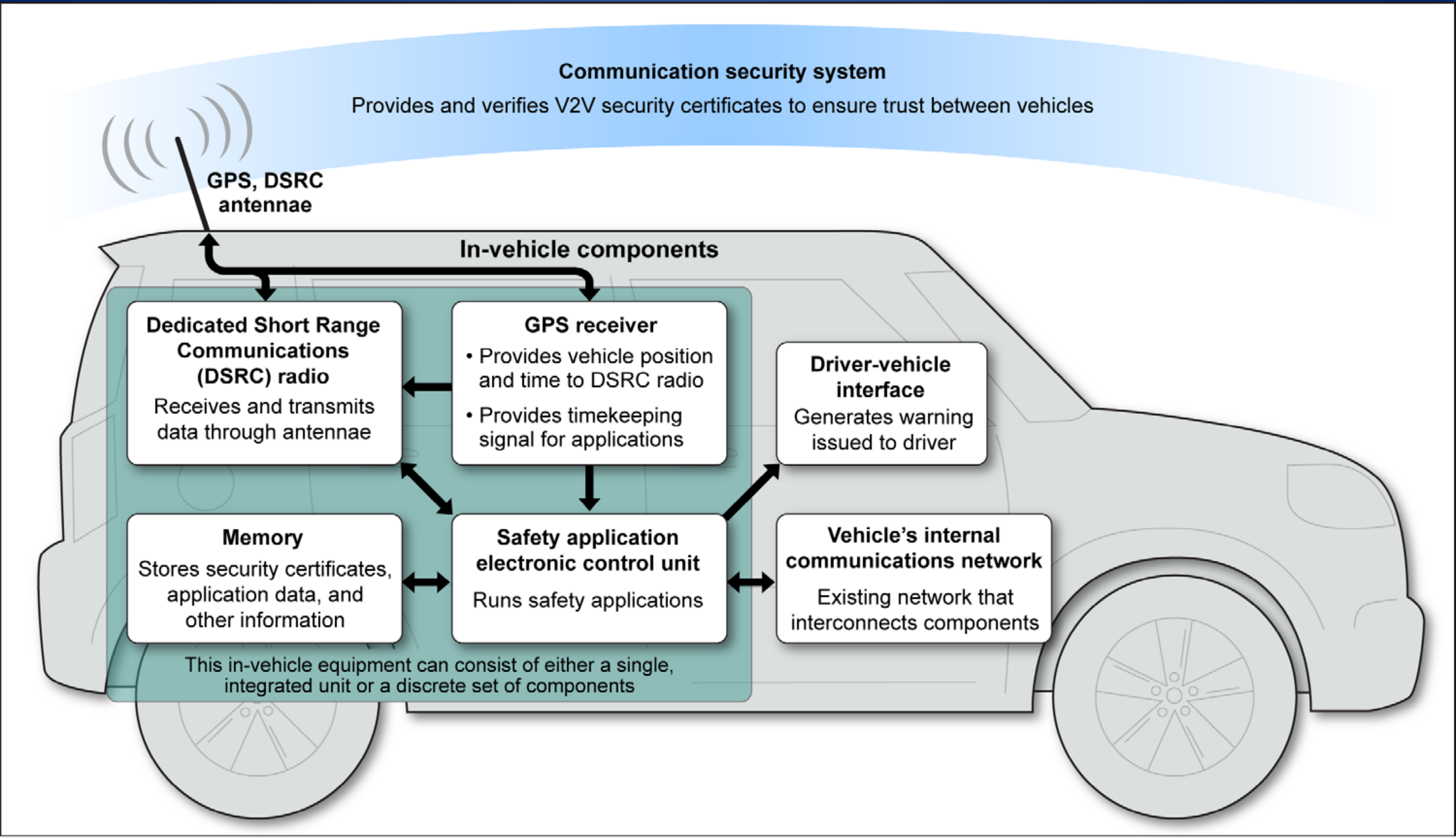
Vehicle Control Information

Transmission State
Brake Status
Steering Wheel Angle
Path History
Path Prediction

Vehicle Information is autonomous and No PII included
Security System

Public Key Infrastructure (PKI)





Sources: Crash Avoidance Metrics Partnership and GAO.

United States Department of Transportation

Office of the Assistant Secretary for Research and Technology

Intelligent Transportation Systems Joint Program Office

Research Areas

Accelerating Deployment
Automation
Connected Vehicles
Emerging Capabilities
Enterprise Data
Interoperability

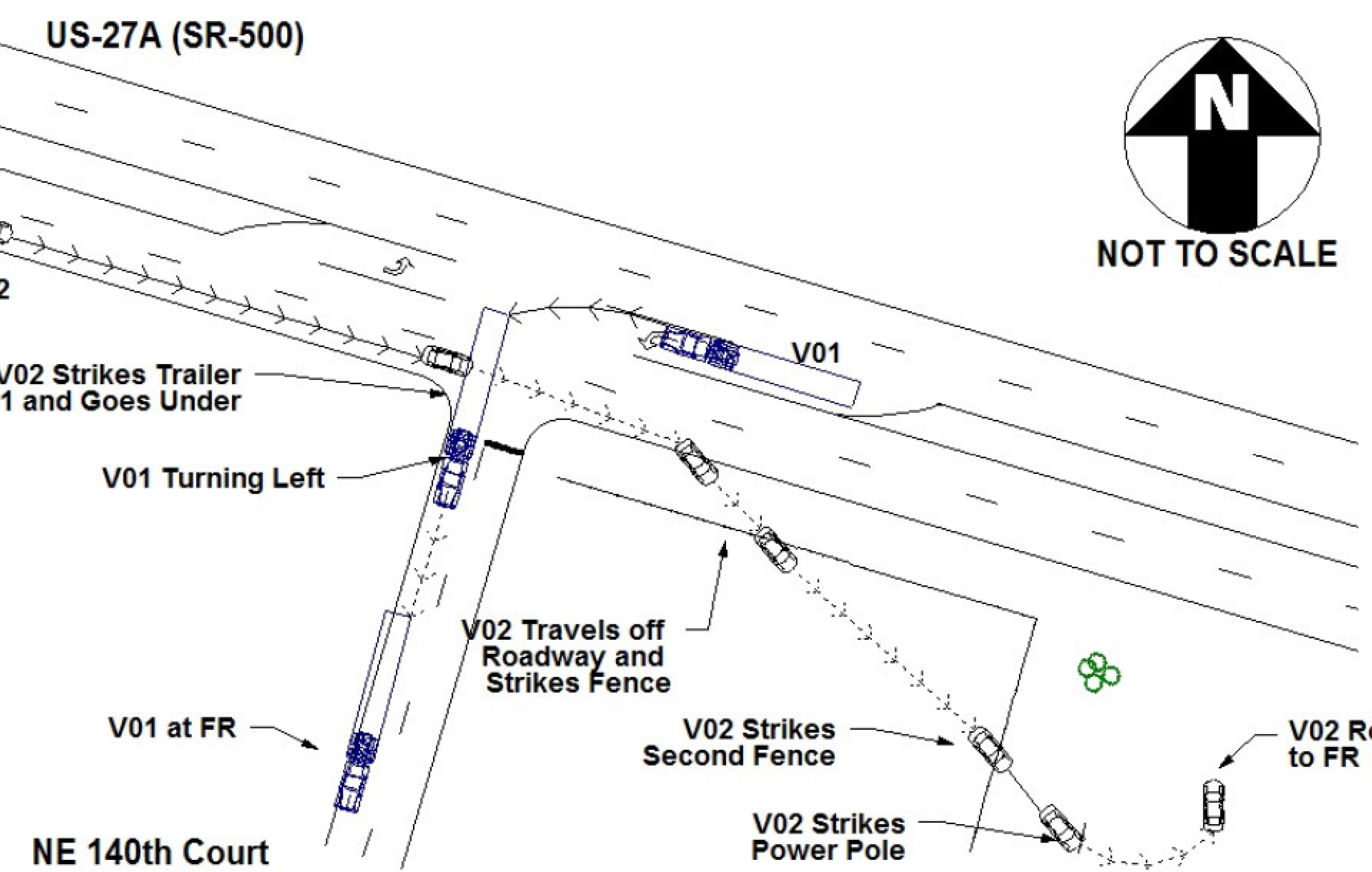
Liability / Insurance

What happens when Technology fails???

Tesla Model S

Fatal Crash
May 7, 2016


66
68°
68°


US-27A (SR-500)
N
NOT TO SCALE
V01
V02 Strikes Trailer
1 and Goes Under
V01 Turning Left
V02 Travels off
Roadway and
Strikes Fence
V01 at FR
V02 Strikes
Second Fence
V02 Strikes
Power Pole
to FR
NE 140th Court

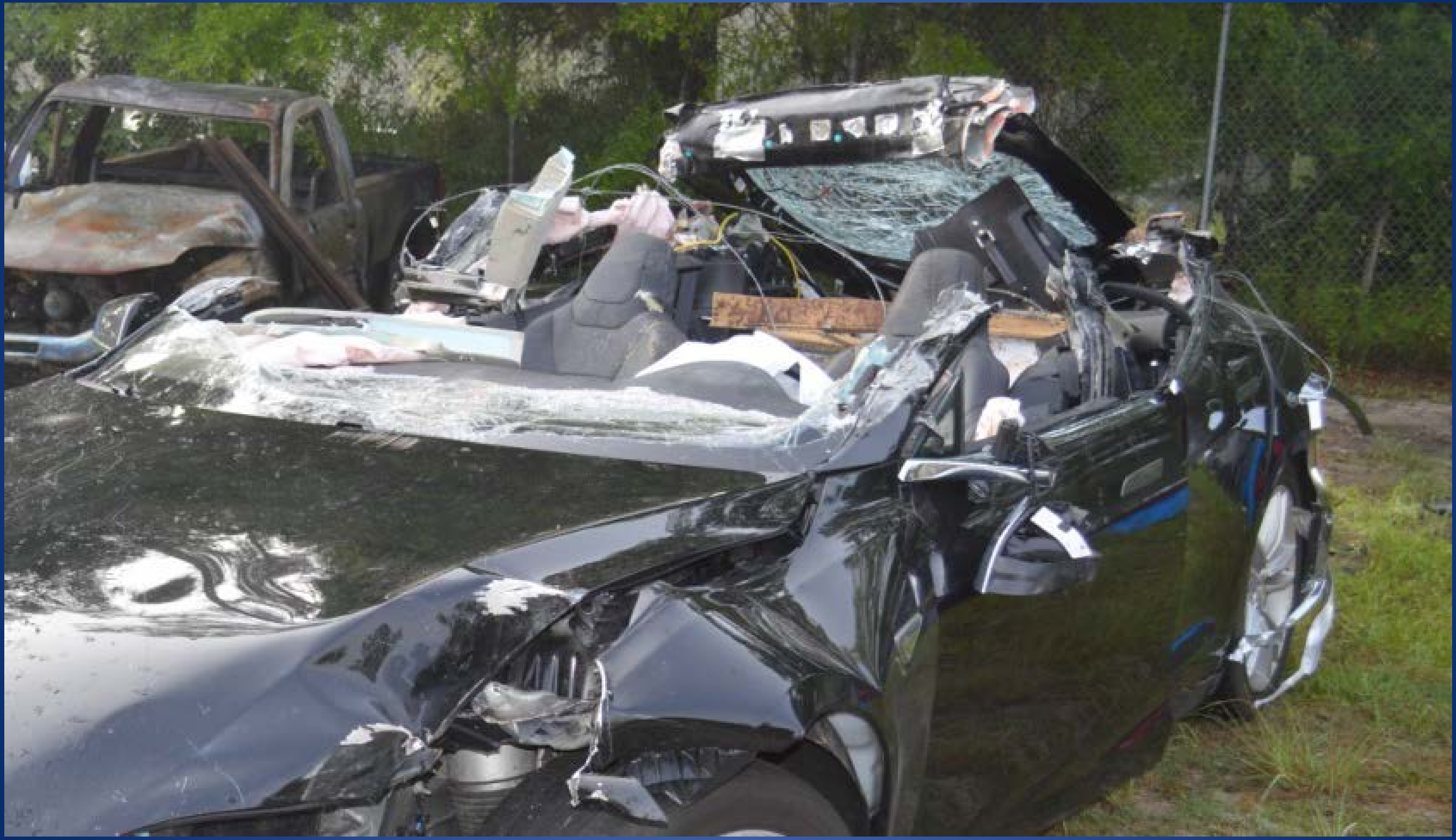


Photo: Florida Highway Patrol

On June 28, 2016, NHTSA opened PE16-007 to
“examine the design and performance of any automated driving systems in use at the time of the crash.

NHTSA’s examination did not identify any defects in the design or performance of the AEB or Autopilot systems of
the subject vehicles nor any incidents in which the systems did not perform as designed.

NTSB Press Release

National Transportation Safety Board Office of Public Affairs
Driver Errors, Overreliance on Automation, Lack of Safeguards, Led to Fatal Tesla Crash
9/12/2017

WASHINGTON (Sept. 12, 2017) — The National Transportation Safety Board determined Tuesday that a truck driver’s failure to yield the right of way and a car driver’s inattention due to overreliance on vehicle automation are the probable cause of the fatal May 7, 2016, crash near Williston, Florida.

NTSB Findings
September 12, 2017

9. The way that the Tesla Autopilot system monitored and responded to the driver's interaction with the steering wheel was not an effective method of ensuring driver engagement.

10. Without the manufacturer's involvement, vehicle performance data associated with highly automated systems on vehicles involved in crashes cannot be independently analyzed or verified.

11. A standardized set of retrievable data is needed to enable independent assessment of automated vehicle safety and to foster automation system improvements.

INSURANCE JOURNAL

Tesla Introduces 'Substantial Improvements' to Autopilot
By Dana Hull | September 12, 2016

Radar images vs. optical camera images

Positive control when Driver ignores warnings

It’s All Over The News……

The Next Cybersecurity Concern: Your Car

Digital Carjackers Show Off New Attacks

Forbes

Subscribe 138,182

Vox

THURSDAY, MARCH 12, 2015

The next frontier of hacking: your car

Updated by Timothy B. Lee on January 18, 2015, 1:00 p... tim@vox.com

Beware! Hackers are eyeing your car’s safety features to extort money

ANI | December 28, 2014, 15.12 pm IST

YouTube

0:51 / 3:24

Car Hacking DARPA

timelinesoon

Subscribe 699

CAR HACKED ON 60 MINUTES

How to Hack a Car: Phreaked Out (Episode 2)

Motherboard

Subscribe 471,837

Report: Cars are vulnerable to wireless hacking

David Shepardson, The Detroit News *10:18 p.m. EST February 8, 2015*

Auto Makers Fall Behind in Anti-Hacking Efforts, Executives in Several Industries Say

February 18, 2015 Tagged With: Car Hacking, Cyber Security, Executive Brief

FOR IMMEDIATE RELEASE
Date: September 30, 2015

VIRGINIA CYBER SECURITY RESEARCH LEADING THE WAY TOWARDS SAFEGUARDING THE NATION'S FIRST RESPONDERS

Public-Private Initiative Showcased at Commonwealth of Virginia Cyber-Security Summit

RICHMOND – Governor Terry McAuliffe announced today the promising results of a collaborative public-private initiative to explore the safeguards needed to protect Virginia's citizens and public safety agencies from cyber security attacks targeting automobiles. Introduced in May, this is one of the first spin-off activities of the Virginia Cyber Security Commission and Virginia Cyber Security Partnership.

This particular public-private working group has spent the past six months working with the Virginia State Police to address the potential for cyber attacks on automobiles, specifically those vehicles used by first responders. The group first focused on the mechanisms of how an attack could be rendered on a police vehicle. Then, a series of trials were conducted last week at the Virginia State Police Training Track Complex to identify and measure the level of awareness that currently exists with public safety personnel in regards to a police vehicle's vulnerability to a cyber attack. The results of the preliminary trials will be used to aid law enforcement agencies and other first responders with establishing training protocols and exploring low-cost technology that can be developed to assist public safety agencies with defending their vehicles against a cyber attack.

An overview of the research was presented and demonstrated today by Dr. Barry M. Horowitz, Chair and Munster Professor of Systems and Information Engineering at the University of Virginia, at the two-day Commonwealth of Virginia Cyber Security – Unmanned Systems Technology Showcase at John Tyler Community College's Chester Campus.

"I applaud our hardworking partners on this important, collaborative cyber security initiative," **Governor McAuliffe said.** "This invaluable research is essential for the Commonwealth to advance its objectives to better safeguard our drivers, their vehicles and, especially, our public safety professionals. The data and protocols derived from this project are some of the first of its kind in the nation, and will be instrumental in facilitating a more universal discussion about mitigating the risks that potentially exist for vehicle fleets of all kinds."

As this work group continues its efforts as part of the Governor McAuliffe's "Cyber Virginia" platform, it will push to further identify and resolve several critically important issues related to protecting Virginians' vehicles and the vehicle fleets operated by law enforcement agencies, to include the following goals:

- Develop strategies for Virginia citizens and public safety personnel to identify and prevent cyber security threats targeting vehicles and other consumer devices.
- Explore the economic development opportunities related to this specialized cyber security field within the Commonwealth.

Virginia
State Police

Automobile
Cybersecurity Project

....and in coordination with:


TROOPER
STATE
POLICE

STATE
POLICE

STATE
POLICE

STATE
POLICE


POLICE
Fire Department
HAZMAT
HAZMAT
POLICE
POLICE
FIRST AID BOX


FATE
OF THE FURIOUS


YOUR COUNTY
SHERIFF
STATE OF LOUISIANA
UNION · JUSTICE
CONFIDENCE
DEPUTY
OH
OFFICER
LICE
TY NAME
CITY OF
OUR CITY NAME
SEAL OF THE STATE OF OHIO
LICE
HIO

"What" do we need to do as public safety professionals to reduce the risks of a cyber attack?

"What" training protocols do we need in place to make certain our personnel can identify a cyber attack if/when it occurs?

"What" practices do we need to add to our personnel's existing safety vehicle checks?

Virginia State Police
Cybersecurity Requirements

ASSESS THE POSSIBILITY OF CYBER-ATTACK.

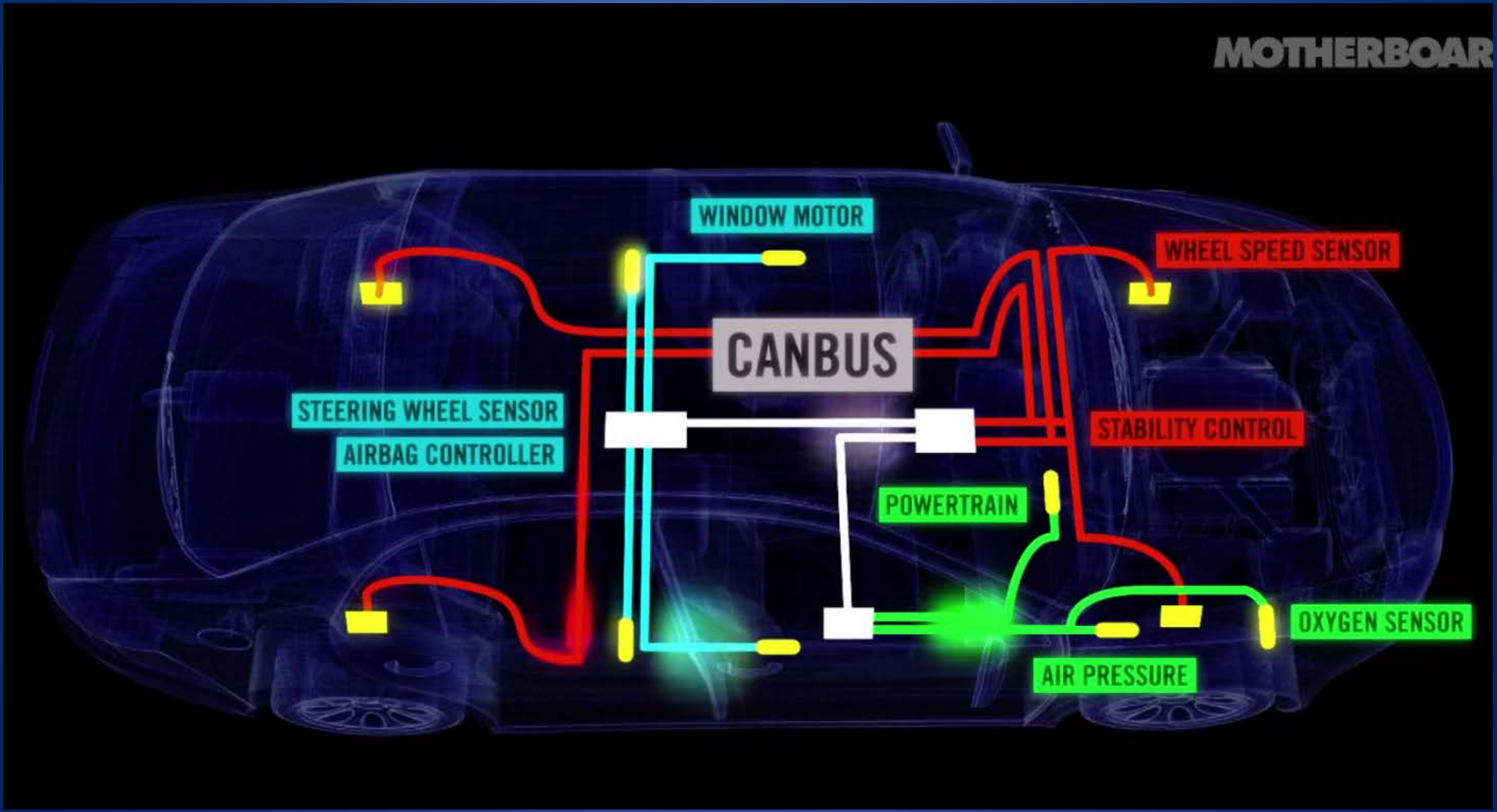
ENSURE THE SECURITY OF POLICE VEHICLE FLEETS.

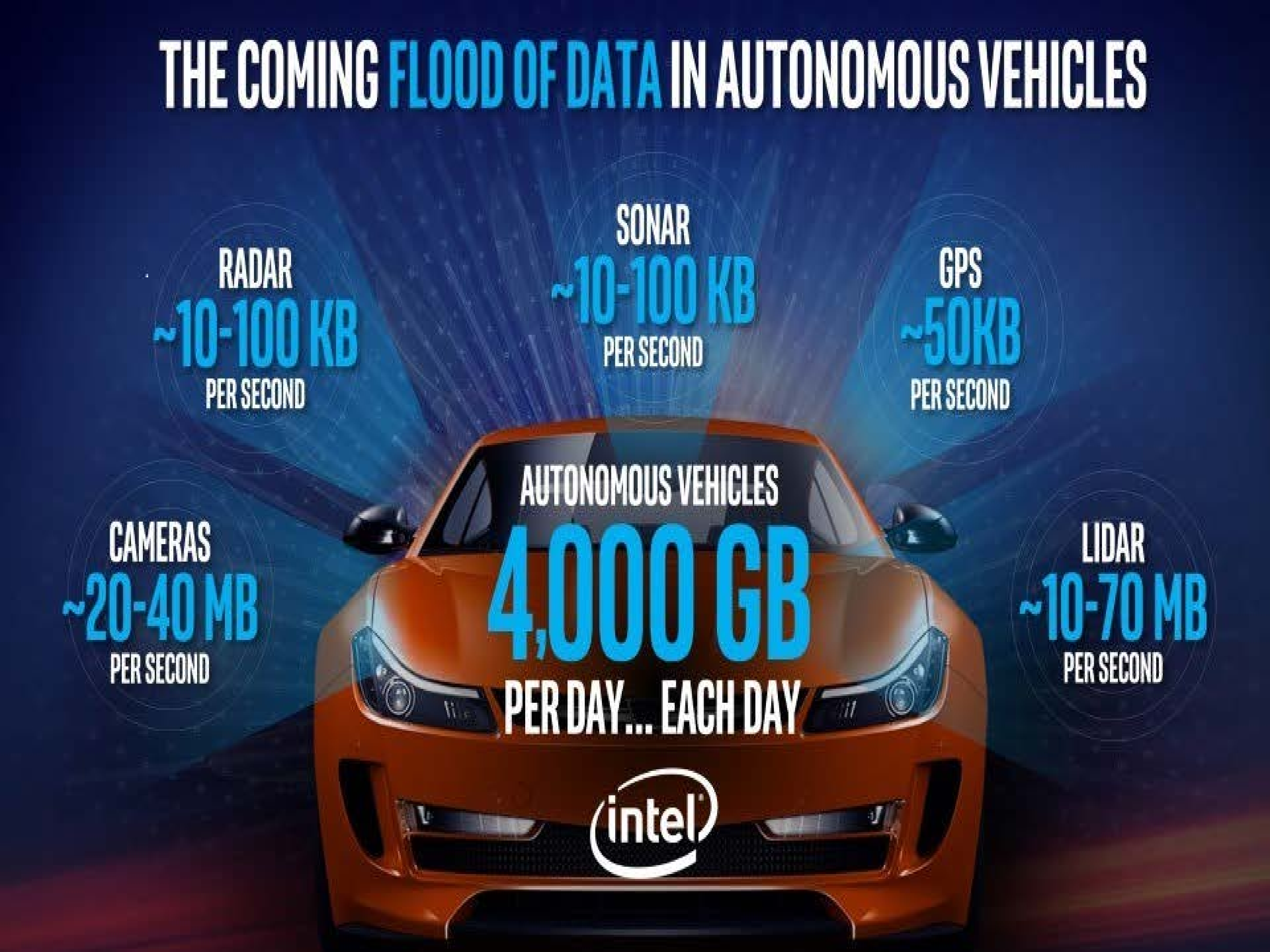
DEVELOP A FORENSIC CAPABILITY TO EXAMINE AND ANALYZE A VEHICLE AT THE SCENE OF AN INCIDENT.

Project Phases – 90 Days

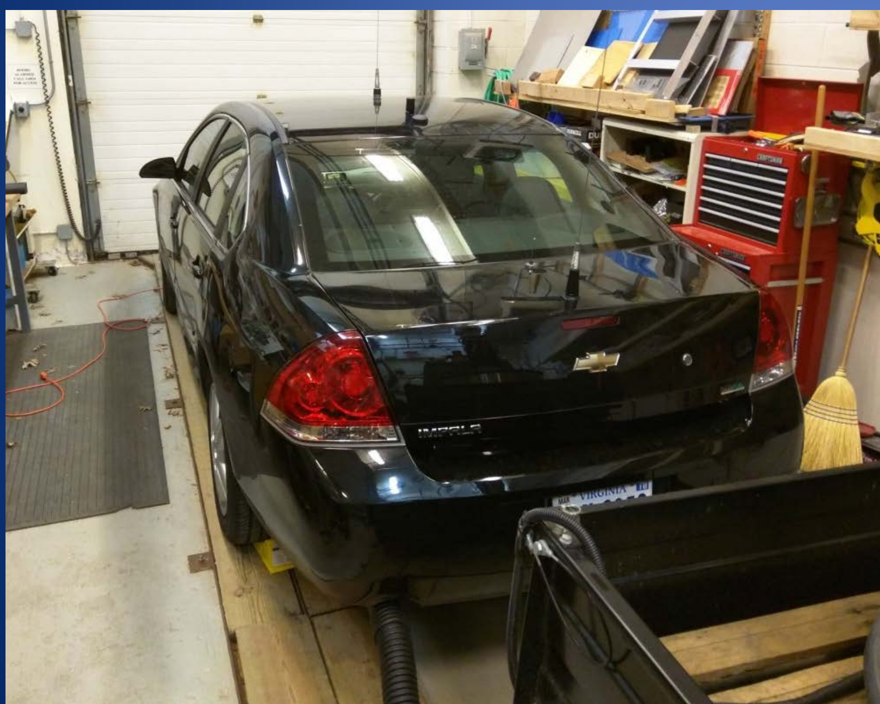
- Phase I – Assessment / Study
- Phase II – Attacks
- Phase III – Solutions / Forensics
- Phase IV - Documentation

Cars Now Contain Lots of Cyber Attack Access Paths




THE COMING FLOOD OF DATA IN AUTONOMOUS VEHICLES
RADAR
~10-100 KB
PER SECOND
SONAR
~10-100 KB
PER SECOND
GPS
~50KB
PER SECOND
CAMERAS
~20-40 MB
PER SECOND
AUTONOMOUS VEHICLES
4,000 GB
PER DAY... EACH DAY
LIDAR
~10-70 MB
PER SECOND
intel


STATE POLICE
POLICE


VIRGINIA


VIRGINIA
XAV-8953


STATE
POLICE
TROOPER

VEHICLE ATTACK	ACTION	CONSEQUENCE
Uncontrolled acceleration to limit	Loss of control	Potential for accident/injury/death to Trooper or civilians
Disengagement of brakes	Loss of control	Potential for accident/injury/death to Trooper or civilians
Asymmetrical braking	Loss of control	Potential for accident/injury/death to Trooper or civilians
Deployment of airbag at speed	Loss of control	Potential for accident/injury/death to Trooper or civilians
Cancellation of all lighting (external & internal) at night	Loss of control	Potential for accident/injury/death to Trooper or civilians
Transmission operation altered	Trooper Stops vehicle	Vehicle removed from service, inability to answer calls
Alter RPM,Throttle, Timing settings	Trooper Stops vehicle	Inability to answer calls for service, vehicle submitted for maintenance
Disengage Electronic Stability Control	Trooper Stops vehicle	Inability to answer calls for service, vehicle submitted for maintenance
Disengage ABS system	Warning Light illuminated	No action required immediately, submitted for service
Shutoff engine no restart	Vehicle stops	Vehicle towed for service, inability to answer calls
Prevent engine from turning off or starting	None	Vehicle removed from service, inability to answer calls

VEHICLE ATTACK	ACTION	CONSEQUENCE
Instrument panel: Falsify readings	Trooper Stops vehicle	No traffic enforcement activity, removed from service
Door Locks activated continuously	None	Inability to answer calls for service, vehicle submitted for maintenance
Unlock Doors	Attempt to secure vehicle	Theft of firearms, radio, and other equipment
Unlock Trunk	Attempt to secure vehicle	Theft of firearms, radio, and other equipment
Lower windows	Attempt to secure vehicle	Theft of property, possible damage from elements
Horn Blows continuously	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Heat / Air conditioning activated continuously	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Car Radio On with increase volume	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Wiper / Washer activated continuously	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Wiping Code	None	No Forensic Investigation capability

PR_17-1327.mp4

Recommendations

- Public Safety personnel should currently receive annual training on cyber awareness.

- Cyber awareness should now include physical systems – police cars, bomb robots, UAV’s, GPS, LPR’s, radio systems, body cams, etc….

Recommendations cont.

- Agency Managers should review / formulate policy for physical inspections of external and internal areas of police vehicles (prior to duty, return from maintenance from 3rd party vendors)
- Inspect OBD-II port beneath dash, any device attached should be treated as suspicious. Vehicle removed from service until cleared.

Recommendations cont.

- IACP currently in preliminary stages of developing a checklist for use by officers as a general guideline for cybersecurity best practices for physical systems.

- Development of lesson plans and training of personnel during initial and Inservice training to generate cyber awareness.

Recommendations cont.

- The “Cyber Crime Checklist for Police Chiefs” by IACP used as baseline reference tool. Obtained through the IACP Cyber Center.
- All agencies should ensure cybersecurity matters are reflected in their public safety mission requirements, and appropriate personnel are designated to maintain SME in the area.

Recommendations cont.

- The Society of Automotive Engineers (SAE) has published Standard J3061;

"Cybersecurity Guidebook for
Cyber-Physical Systems"

This guide addresses cybersecurity threats and identifies minimum standards necessary to secure vehicle systems.

Recommendations cont.

- Participate in the DHS Government Vehicle Cybersecurity Steering Committee. Bi-monthly teleconferences to develop actionable information on cyber issues for vehicles operated by governmental entities.

- Review existing criminal statutes for applicability to physical systems.

Recommendations cont.

- Agencies should partner with the automotive industry, public / private cybersecurity companies, and academia to further research and development.
- A critical need is for forensic capability at the scene of an incident for data extraction and analysis.
- New policy creation regarding cybersecurity.

Recommendations cont.

- Consider reallocation of current patrol assignments to community policing / emergency response roles
- How will reduction in revenue impact services?
- Technical vs. Tactical skills
- Use of technology as a force multiplier

CAPTAIN JERRY DAVIS
VIRGINIA STATE POLICE - WYTHEVILLE
JERRY.DAVIS@VSP.VIRGINIA.GOV
(276) 223-4241