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
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

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

---


20 INDUSTRIES AUTONOMOUS VEHICLES WILL DISRUPT BY 2025

Enacted Autonomous Vehicle Measures
Source: National Conference of State Legislators
# Great Mileage
Some Benefits of the Driverless Car

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

Sources: Google, US NHTSA, AAA, Texas A&M Transportation Institute, Columbia University Earth Institute and Devil’s Advocate Group’s analysis
A Combination of Sensors Enable Autonomous Vehicle Capabilities

**Lidar:** Rotating or fixed laser-based sensors create a continuously updating high-resolution 3D map, detecting edges of road, lane markings, and obstacles, but is susceptible to interference from rain, fog, and smoke.

**GPS and gyroscopes:** Localization of the car, using a combination of satellite-based GPS along with on-vehicle sensors for improved accuracy.

**Optical cameras:** Front view and rear view cameras complement other sensors by detecting colors in traffic lights and road signs, and help detect pedestrians and obstacles.

**Radar:** Multiple radar units in the front and rear are low cost and excel at providing precise speed information about surrounding cars, but have lower resolution than lidar for obstacle detection and mapping.

*Source: Lux Research, Inc.*

www.luxresearchinc.com
Sensing system components and effective ranges.
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0</td>
<td>The human driver is in complete control of all functions of the car</td>
</tr>
<tr>
<td>Level 1</td>
<td>One function is automated</td>
</tr>
<tr>
<td>Level 2</td>
<td>More than one function is automated at the same time, but the driver remains attentive</td>
</tr>
<tr>
<td>Level 3</td>
<td>Driving functions are sufficiently automated - the driver can safely engage in other activities</td>
</tr>
<tr>
<td>Level 4</td>
<td>The car is self-driving - no human driver required</td>
</tr>
</tbody>
</table>
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
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
FULLY AUTOMATED
Monitoring of the system not required
Driver does not need to be able to take over the driving task
Example: Highway driving up to 130 km/h

HIGHLY AUTOMATED
Monitoring of the system not required
Driver needs to be able to take over the driving task with lead time
Example: Stop-and-go (highway)

PARTIALLY AUTOMATED
Monitoring of the system required
Driver needs to be able to take over the driving task at any moment
Example: Shop-and-go up to 30 km/h
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)
Vehicle to Mobile Devices
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
<table>
<thead>
<tr>
<th>Scenario and warning type</th>
<th>Scenario example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rear end collision scenarios</strong></td>
<td></td>
</tr>
<tr>
<td>Forward collision warning</td>
<td>Approaching a vehicle that is decelerating or stopped.</td>
</tr>
<tr>
<td>Emergency electronic brake light warning</td>
<td>Approaching a vehicle braking hard or stopped in roadway but not visible due to obstructions.</td>
</tr>
<tr>
<td><strong>Lane change scenarios</strong></td>
<td></td>
</tr>
<tr>
<td>Blind spot warning</td>
<td>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.</td>
</tr>
<tr>
<td>Do not pass warning</td>
<td>Encroaching onto the travel lane of another vehicle traveling in opposite vehicle direction.</td>
</tr>
<tr>
<td><strong>Intersection scenario</strong></td>
<td></td>
</tr>
<tr>
<td>Intersection warning</td>
<td>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.</td>
</tr>
</tbody>
</table>


Source: GAO analysis of Crash Avoidance Metrics Partnership information.
Target Unimpaired Light Vehicle Crashes Potentially Addressed by V2V

- 19% Target LV Unimpaired Crashes
- 81% Remaining LV Crashes

Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application
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)
Communication security system
Provides and verifies V2V security certificates to ensure trust between vehicles

GPS, DSRC antennae

In-vehicle components

Dedicated Short Range Communications (DSRC) radio
Receives and transmits data through antennae

GPS receiver
- Provides vehicle position and time to DSRC radio
- Provides timekeeping signal for applications

Memory
Stores security certificates, application data, and other information

Safety application electronic control unit
Runs safety applications

Driver-vehicle interface
Generates warning issued to driver

Vehicle’s internal communications network
Existing network that interconnects components

This in-vehicle equipment can consist of either a single, integrated unit or a discrete set of components

Sources: Crash Avoidance Metrics Partnership and GAO.
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
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

NE 140th Court
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.
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.
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.
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

Vox

THURSDAY, MARCH 12, 2015

The next frontier of hacking: your car

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

ANI | December 28, 2014, 15:12 pm IST

CAR HACKED ON 60 MINUTES

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

Motherboard

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

[Images of hacking and cars]

[Images of hacking and cars]
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:

U.S. Department of Transportation
Volpe, The National Transportation Systems Center
“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: ~50 KB per second
- Cameras: ~20-40 MB per second
- LIDAR: ~10-70 MB per second

Autonomous Vehicles: 4,000 GB per day... each day
<table>
<thead>
<tr>
<th>VEHICLE ATTACK</th>
<th>ACTION</th>
<th>CONSEQUENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncontrolled acceleration to limit</td>
<td>Loss of control</td>
<td>Potential for accident/injury/death to Trooper or civilians</td>
</tr>
<tr>
<td>Disengagement of brakes</td>
<td>Loss of control</td>
<td>Potential for accident/injury/death to Trooper or civilians</td>
</tr>
<tr>
<td>Asymmetrical braking</td>
<td>Loss of control</td>
<td>Potential for accident/injury/death to Trooper or civilians</td>
</tr>
<tr>
<td>Deployment of airbag at speed</td>
<td>Loss of control</td>
<td>Potential for accident/injury/death to Trooper or civilians</td>
</tr>
<tr>
<td>Cancellation of all lighting (external &amp; internal) at night</td>
<td>Loss of control</td>
<td>Potential for accident/injury/death to Trooper or civilians</td>
</tr>
<tr>
<td>Transmission operation altered</td>
<td>Trooper Stops vehicle</td>
<td>Vehicle removed from service, inability to answer calls</td>
</tr>
<tr>
<td>Alter RPM, Throttle, Timing settings</td>
<td>Trooper Stops vehicle</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Disengage Electronic Stability Control</td>
<td>Trooper Stops vehicle</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Disengage ABS system</td>
<td>Warning Light illuminated</td>
<td>No action required immediately, submitted for service</td>
</tr>
<tr>
<td>Shutoff engine no restart</td>
<td>Vehicle stops</td>
<td>Vehicle towed for service, inability to answer calls</td>
</tr>
<tr>
<td>Prevent engine from turning off or starting</td>
<td>None</td>
<td>Vehicle removed from service, inability to answer calls</td>
</tr>
<tr>
<td>VEHICLE ATTACK</td>
<td>ACTION</td>
<td>CONSEQUENCE</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Instrument panel: Falsify readings</td>
<td>Trooper Stops vehicle</td>
<td>No traffic enforcement activity, removed from service</td>
</tr>
<tr>
<td>Door Locks activated continuously</td>
<td>None</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Unlock Doors</td>
<td>Attempt to secure vehicle</td>
<td>Theft of firearms, radio, and other equipment</td>
</tr>
<tr>
<td>Unlock Trunk</td>
<td>Attempt to secure vehicle</td>
<td>Theft of firearms, radio, and other equipment</td>
</tr>
<tr>
<td>Lower windows</td>
<td>Attempt to secure vehicle</td>
<td>Theft of property, possible damage from elements</td>
</tr>
<tr>
<td>Horn Blows continuously</td>
<td>Remove vehicle from service</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Heat / Air conditioning activated</td>
<td>Remove vehicle from service</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Heat / Air conditioning activated</td>
<td>Remove vehicle from service</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Car Radio On with increase volume</td>
<td>Remove vehicle from service</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Wiper / Washer activated continuously</td>
<td>Remove vehicle from service</td>
<td>Inability to answer calls for service, vehicle submitted for maintenance</td>
</tr>
<tr>
<td>Wiping Code</td>
<td>None</td>
<td>No Forensic Investigation capability</td>
</tr>
</tbody>
</table>
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.
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