Idaho Autonomous Vehicle And Connected Vehicle

Testing and Deployment Committee

Welcome!

Brian Ness

Director, Idaho Transportation Department

May Minutes

- **Approve Meeting Minutes**

First Report to the Governor

- **Due to Governor's Office:** November 1, 2018

- **Next Meetings:** October 16, 2018

  — Then as required

Committee Focus

Idaho:

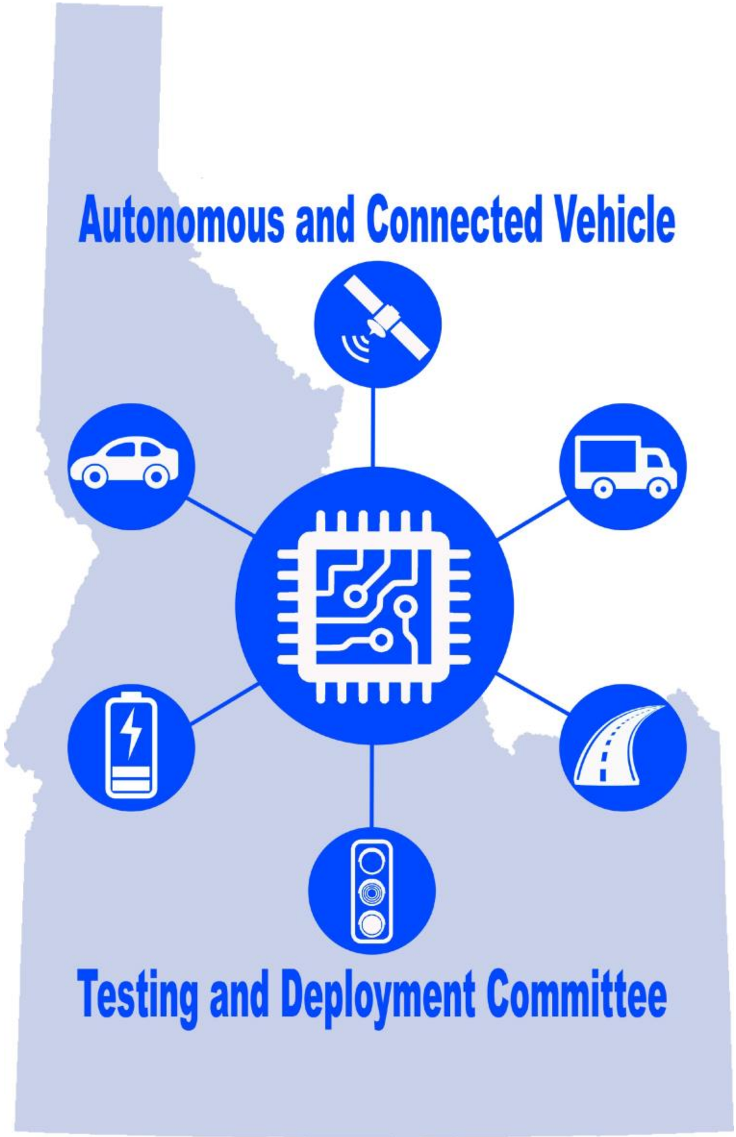
Autonomous and Connected Vehicles

AASHTO:

Cooperative Automated Transportation (CAT)

Focus Areas

- State/Federal Activity
- Safety and Infrastructure
- **Security and Privacy**
- **Testing and Deployment**



Video Placed Here for Meeting Only

Idaho Autonomous Vehicle And Connected Vehicle

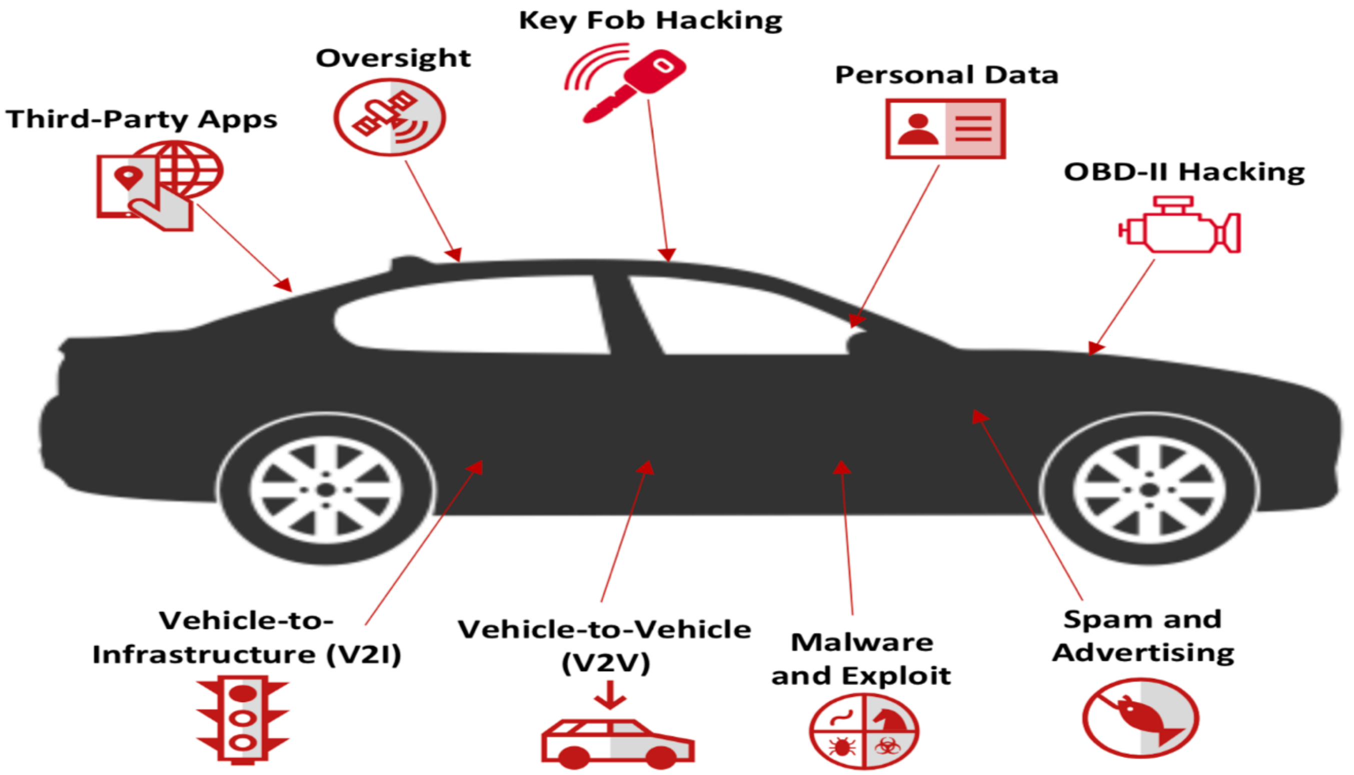
Testing and Deployment Committee

System Infrastructure

Pete Palacios

Idaho Transportation Department

The digital infrastructure for connected and autonomous vehicles



The Language

- **Cellular – Mobile radio telephone**

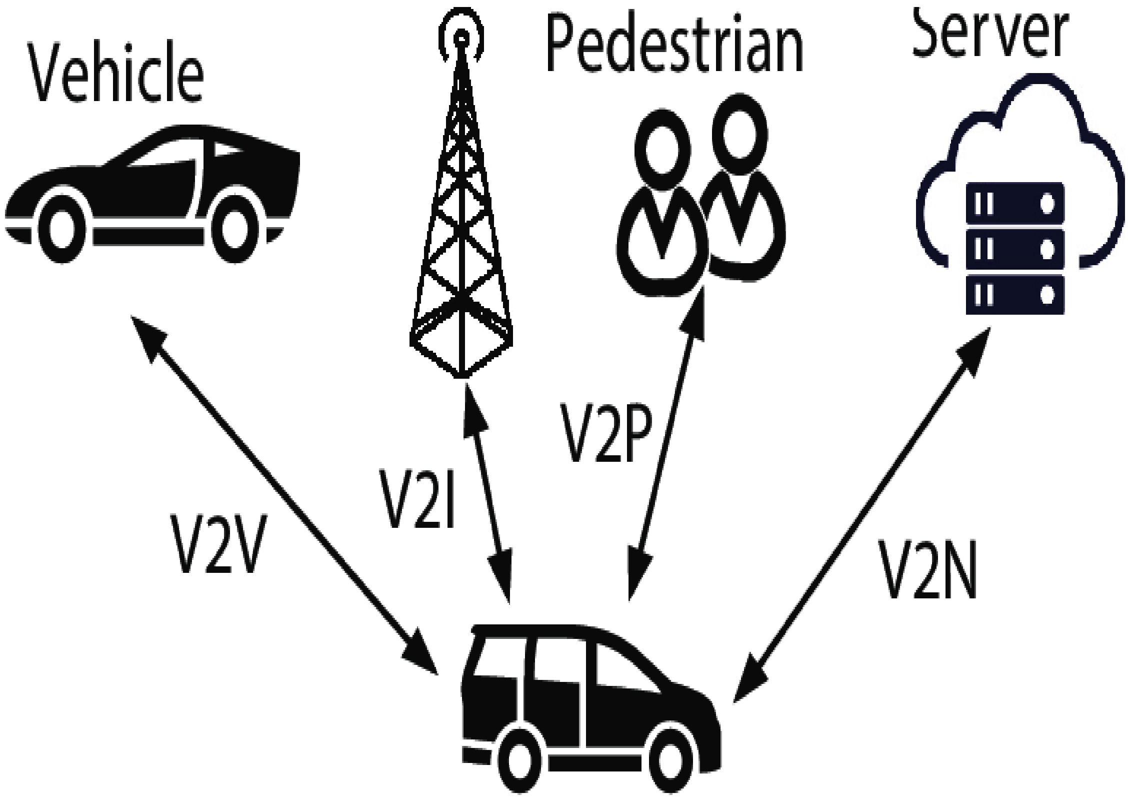
- **Wi-Fi – Branding for IEEE 802.11x standard for high speed wireless communications**

- **Dedicated Short Range Communications (DSRC) – short or medium range communication channels designed for automotive use.**

- **SAEs Classifications**

The vehicles

- **Vehicle Manufacturers developing “independent” vehicles**
- **Estimated 25 gigabytes of data uploaded every hour**
- **Communicate with what is available**
- **Multi-mode – connect via any of the technologies as needed.**



What data should a government transportation entity provide?

Over the road

- Port of Entry
- Workzones
- Safety alerting
- Intelligent location

Metro travel

- Workzones
- Traffic flow
- Safety alerting
- Intelligent location

What to prepare for.

Determine what data should be provided

Determine how we collect that data

Design and plan the digital infrastructure to make data available.

Idaho Autonomous Vehicle And Connected Vehicle

Testing and Deployment Committee

System Infrastructure

Discussion

Idaho Autonomous Vehicle And Connected Vehicle

Testing and Deployment Committee

Cyber Security and Data Privacy

Ken Rohde

Idaho National Laboratory

Cyber Security Considerations for Electric and Autonomous Vehicles

2018 Idaho Autonomous and Connected Vehicle Testing and Deployment Committee

AUGUST 21, 2018

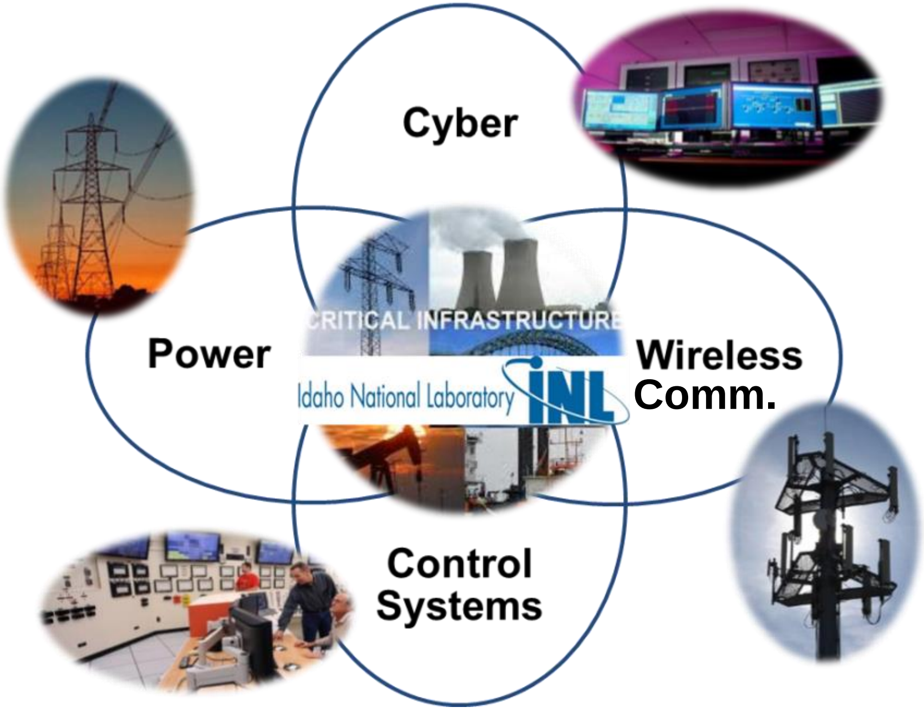
Ken Rohde – Cyber Security R&D
Cybercore Integration Center

INL/LTD-18-51153

www.inl.gov

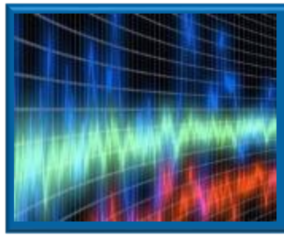
Idaho National Laboratory

Cyber Security Programs



Nuclear safety and security

Secure and resilient electric grid



Wireless security and spectrum crunch

Secure industrial control systems across critical infrastructure sectors

Cyber Security Timeline

2003 → 2018+

DOE OE → DHS CSSP → Industry Partners → Work for Others → LDRD → DOE EERE



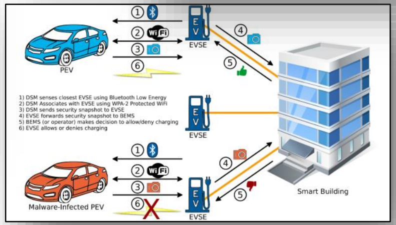


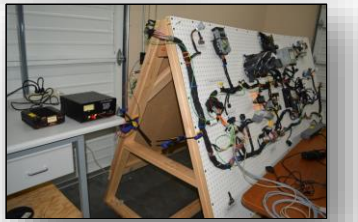










What Does Cyber Security Mean?

- Protection of digital systems from unauthorized or unintended use
- Protection of digital data
- Protection of physical systems connected to digital controls
- Protection of “critical infrastructure”

- Engineering design to mitigate potential impacts of cyber influence
- Analysis and education of how systems should be deployed

A combined team of experts in their field who understand the potential harm that might be caused as a result of successfully exploited vulnerabilities

What Is A Vulnerability?

- A quality or state of being exposed to the ***possibility*** of being attacked or harmed, either physically or emotionally (dictionary)
  - Unencrypted sensitive data
  - Buffer overflows
  - Missing guards on a table saw
  - No GFCI outlet near the pool
  - Disgruntled employees

What Is An Exploit?

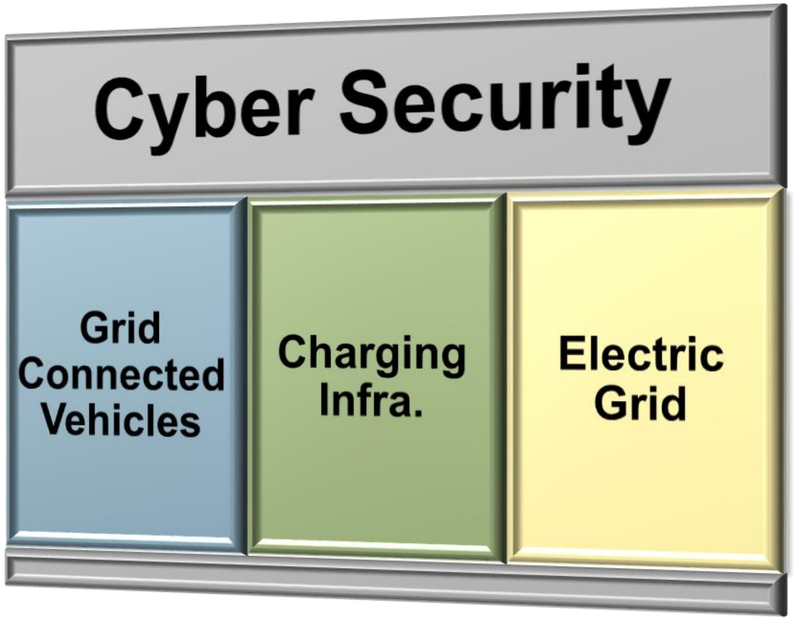
- To make use of and derive benefit from a resource (dictionary)
  - Ransomware
  - Code Red
  - Email phishing
  - Loss of power
  - Loss of life

Not all vulnerabilities are exploitable!

Cyber Informed Engineering

Combining Expertise and Capabilities

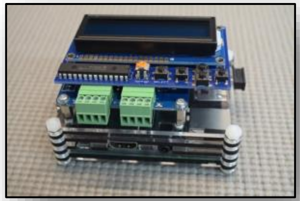
- Advanced Vehicles
  - EV Infrastructure lab (EVIL)
- Cyber Security R&D
  - Hardware Exploitation lab (HEX)
- Power & Energy Systems
  - Real Time Digital Simulation (RTDS)

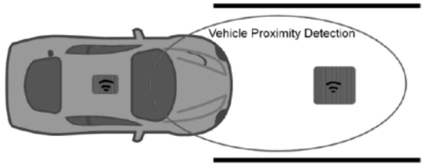


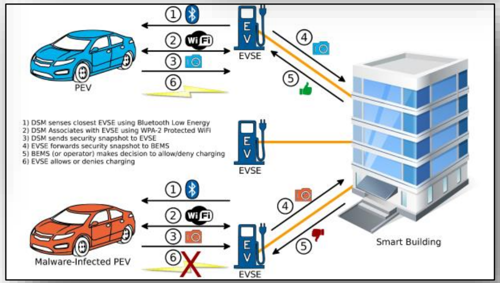
<u>Team Capability</u>: Identify and mitigate PEV charging infrastructure vulnerabilities capable of compromising grid distribution resiliency

Charging Infrastructure Cyber Security

- Conductive Charging
  - AC and DC power transfer
- Inductive Charging
  - Stationary and dynamic
- Medium and Heavy Duty Trucks
- Integration with Smart Grid
- Integration with Micro-Grid and Buildings
- Wireless Communications
  - V2X, DSRC, etc.







Electric Vehicle Infrastructure Laboratory

- Testing and system characterization of
  - Wireless Power Transfer (WPT)
  - Conductive Charging Systems
    - EVSE
    - On-board charger
    - DC Fast Charging

- System performance, efficiency, and safety

- Interaction with and response to grid characteristics and anomalies

- Cybersecurity vulnerability assessment

- Wide range of power capability
  - 1200 kVA capacity
  - Grid Emulator enables dynamic grid event testing

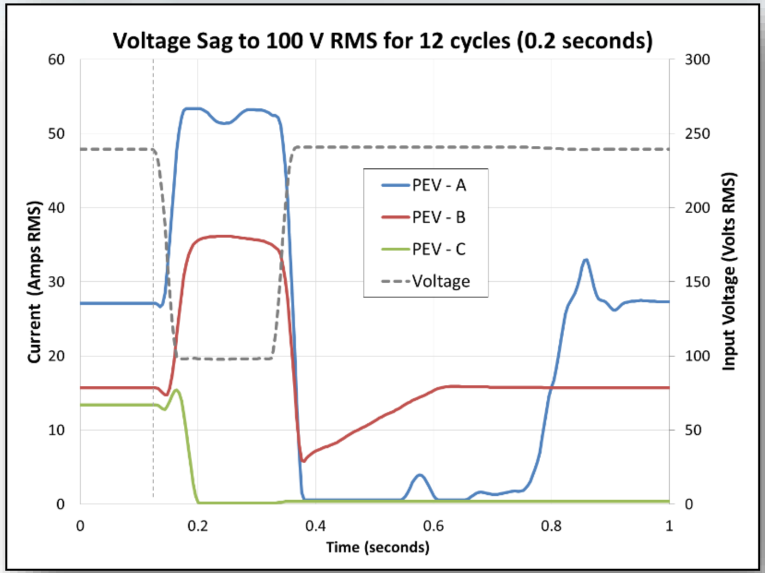
https://avt.inl.gov/panos/EVLTour/?startscene=pano5141

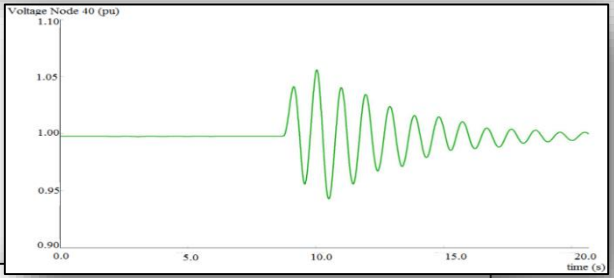
Grid Interaction and Impacts

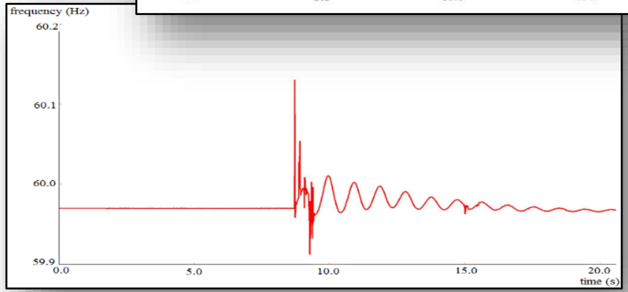
Example: Natural Dynamic Response

- PEV's exposed to a grid voltage sag
  - Result: 2x increase in current draw

- RTDS emulation of 4,000 PEVs
  - Result: grid distribution oscillation







Understanding risks from vulnerabilities

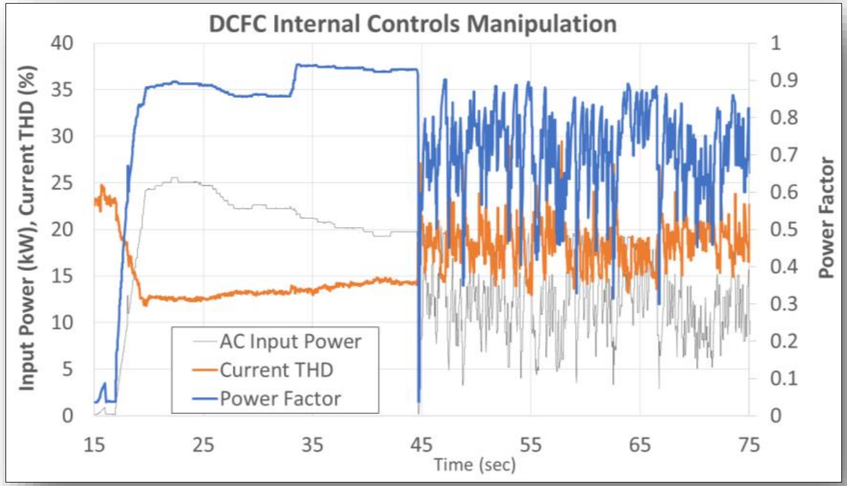
- Dynamic response is exploitable:
  - Wide spread grid disturbance
  - Increase current draw
    - Makes bad condition even worse

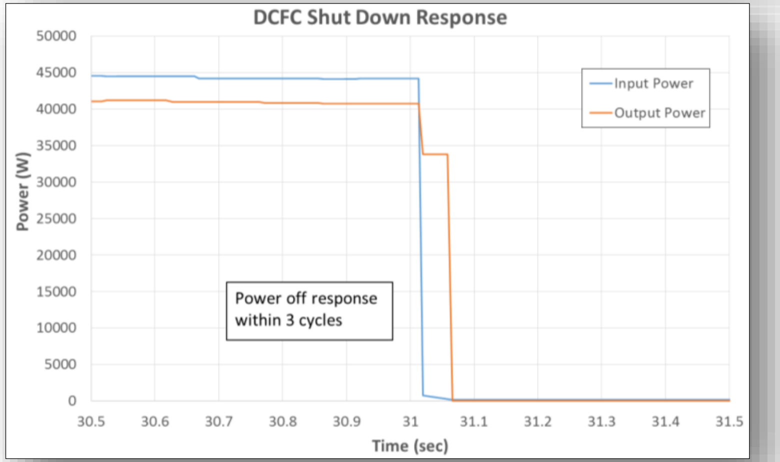
Grid Interaction and Impacts

Example: Cyber Manipulation

- DCFC control system manipulated by cyber methods
  - Impacts to power quality and THD
  - Immediate stopping of power transfer

- Future work will model this across hundreds of charging stations and vehicles

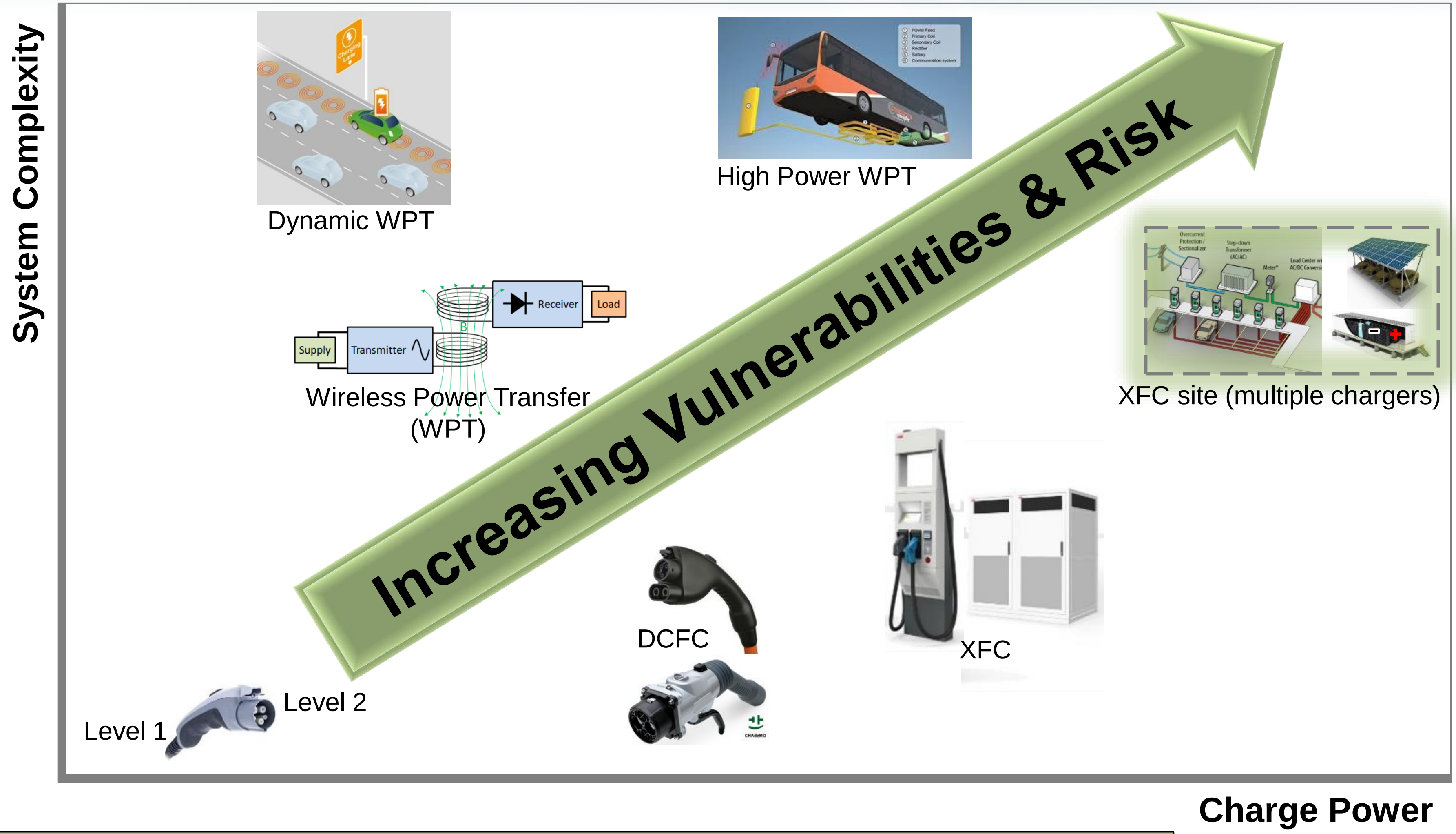




“With great power comes…”

- With higher complexity comes more vulnerabilities
- Autonomous vehicles will raise the bar significantly
  - F-22 Raptor – 2 million
  - Boeing 787 – 7 million
  - 2006 Ford GT – 10 million
  - 2016 Ford F150 – 150 million
  - Autonomous Vehicle – a plethora!
- A more complex infrastructure is also required

Vulnerabilities and Risk



Increased Charge Power and System Complexity results in Increased Vulnerabilities and Risk

Security and Privacy

1. **C**onfidentiality
2. **I**ntegrity
3. **A**vailability

- This model is predominant in traditional information networks
- The primary goal is to keep information private and have a reasonable level of trust in the information received

Security and Privacy

1. Availability

2. Integrity

3. Confidentiality

- The order gets changed in control system environments
- What about when these environments start to mix?

What About PCI and PII?

- Payment Card Industry (PCI) Security Standards
  - PCI Data Security Standard
  - PCI PIN Entry Device Security Requirements
  - PCI Payment Application Data Security Standards

- Personally Identifiable Information (PII)
  - Sensitive Personal Information (SPI)
  - Controlled Unclassified Information (CUI)
  - Confidential Data

Examples Of Failed Privacy

- Bluetooth tethering cellphones to automobiles
- Storing logon credentials locally on IOT devices
- Storing payment information
- Sharing sensitive data, even when it doesn’t appear sensitive
- Tracking aircraft, trucks, busses as they cross the country

General Infrastructure Vulnerabilities

- Physical security of devices is often very poor
  - Zombies Ahead!
- Devices that handle payment information occasionally cache data locally
- Integration with management networks often lack security mechanisms
- Encryption is often deployed poorly
  - Old or vulnerable protocols, poor key management
- Sensitive data needs to be protected from end-to-end but also carefully shared
  - Do you want people to know where ***all*** of your trucks are going?
- Wireless communications must be secure

Closing Thoughts

- Everyone is responsible for security (even cyber security)
- Train all members involved in the effort about the potential issues
- Develop a “consequence driven” engineering and design mindset
- Create a cyber team of those involved in adding infrastructure to ID

Testing and Deployment Focus Area

Idaho Autonomous Vehicle And Connected Vehicle

Testing and Deployment Committee

Training / Licensing / Registration

Amy Smith

Idaho Transportation Department

Idaho AV and CV Testing and Deployment Committee

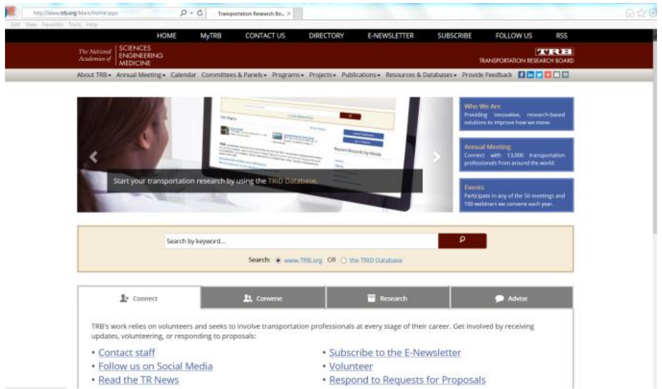
- AV Symposium
- Keynote Speaker – Secretary Elaine Chao
- Lessons to learn
- What needs to happen
- Desired outcomes
- What might change
- Automate CMVs
- Drivers and Vehicles
- Vehicle registration
- Liability issues
- Challenges ahead

Amy Smith, DMV Policy Analyst, Idaho Transportation Department

Who’s Driving? Autonomous Vehicle Symposium – July 2018

- **Sponsored by AUVSI and TRB; more than 1600 attendees from over 30 countries and more than 35 states, over 35 breakout sessions, and 1.5 days of general sessions**

- **Representation from: automakers, technology providers, engineers, academia, government, law enforcement, special interest groups**



Who’s Driving? Keynote Speaker – Secretary Elaine Chao

- Keynote: First and main priority for everyone to remember is “SAFETY”
- AVs must prove to be at least as safe as human drivers or safer, with the overall goal to reduce crashes and save lives
- First steps to deployment must be made wisely and well thought out
- Audience should think about where AV’s add most value
- What do consumers want and demand from AV technology?

Who’s Driving? Key Secretary Points continued

- **NHTSA has released two versions of voluntary guidance for AV providers; version 2.0 late last fall; newer version coming this fall**

- **NHTSA website allows providers to complete a voluntary safety assessment of their technology**

- **The answer to successful deployment is educating the public about AVs and the limitations of the technology**

Who's Driving? Key Secretary Points continued

- **Vitally important to educate the public and provide realistic expectations of this new technology at each level**

- **Both federal and state governments have roles:**
  - **Feds set minimum safety standards of vehicles**
  - **States regulate vehicle operation by registering and licensing drivers.**

Who’s Driving? Lessons to learn

- **States are expected to develop the best approach for them in the implementation of testing and deployment of automated vehicles!**

- **There are many more questions than answers: Manufacturers, technology providers, federal government, state government (including law enforcement, DMVs, Highways), and the insurance industry must work together to set policies**

Who’s Driving? Lessons to learn continued

- **Biggest challenges for automakers/technology, is programming artificial intelligence (AI); How do you program ethics and non verbal queues?**

- **What communication, cybersecurity, common software language and platforms promote uniformity to ease learning use of the technology?**

- **Ensuring performance updates on vehicle technology, software application to keep automated vehicle features current**

Who's Driving? Lessons to learn continued

- Common communication platforms, currently dedicated use of 5.9 mhz
- Disclosure and sharing between manufacturers and developers that reduce risks and enhance security for the public is critical
- NHTSA would like to get safe/secure and innovative solutions to market once considerations of benefits, risks, and transparency has occurred among providers
- Challenge: Does it add value, mobility options to users, make us safer, reduce crashes and save lives?

Who’s Driving? What needs to happen:

- **US DOT Automated Vehicle Research activities identify safety is integral and is a vital key to automating vehicles**
- **Government must modernize regulations and standards; however, this goal is very slow moving through US Congress and federal agencies**
- **Must be able to provide consumer assurance with automated vehicles, that they can get from points A to B, safely and efficiently, as either the “driver” or “occupant”**
- **Manufacturers and technology providers must prove they can achieve this level of safety to increase consumer confidence.**

Who’s Driving? Desired Outcomes

- **Consumers will feel safer when there is government regulation around automated vehicles**
- **Until automated vehicle technology can prove AVs are safer than human driven vehicles, skepticism by the public will continue**
- **General consensus: it will be at least a decade or longer before market penetration of level 2 and 3 vehicles into the country’s mixed vehicle fleet**
- **Some say it will be at least 2050 before level 4 and 5 vehicles make market penetration, due to artificial intelligence programming requirements**

Who’s Driving? Desired Outcomes continued

- **Special attention given to ensuring safety for vulnerable road users (VRU), and should be at the top of the programming priorities**
- **AVs have many sensors/cameras/lidar/radar for communicating with infrastructure and other vehicles; only limited by their capabilities, infrastructure and surroundings**
- **Infrastructure improvements will be paramount to the success of AV deployment, e.g. clear lines and signs will improve the operation of Avs**
- **Human drivers limited by what we can see and experience; reaction time and evasive actions are intuitive; automation has to improve as AVs learn lessons to behave more like human drivers.**

Who’s Driving? Other points

- **Many discussions around deployment and ownership of AVs: will they be owned by fleets, or private citizens?**
- **Once ready for market, costs will be high, resulting in a smaller customer base for purchasing such vehicles**
- **Manufacturers or ridesharing industries may purchase in fleets, and provide Mobility as a Service (MaaS) with a simple app on your phone (currently being tested in Las Vegas)**
- **To be successful as a MaaS, costs must be as similar to ride share or public transportation**

Who’s Driving? Other points continued

- May result in slower market growth, until vehicle fleet turnover allows availability of newer models and customer demand drives costs down

- Many presentations focused on how AVs can provide MaaS to disabled persons who are unable to access public transportation

- Possibly can provide affordable services to the disadvantaged, elderly and school children as a MaaS, when public transportation is far away or unavailable

- MaaS must offer reliable and available service from point A to B, to help these segments of society reach critical services, schools and employment

Who’s Driving? What might change

- Should consider mobility services for all different segments of society, and what mobility may mean to them

- These services could open a world of possibilities to those dependent on others or those outside of public transportation service areas

- Could mean new means to get to/from: services; employment schools; medical appointments; stores; and the bank; many now take for granted

- This technology has the promise to resolve some of the country’s biggest transportation challenges, including access, congestion, flexibility, etc.

Who’s Driving? Automated CMVs

- CV and AV commercial vehicles will bring a revolution of change and opportunities for commercial drivers and carriers; allowing safer operation and reducing the physical and psychological stress for drivers
- These changes alone has benefits; making moving goods much more safe and efficient, especially combined with platooning vehicles
- Changes may also help to address the shortage of commercial drivers, as more retire, with not as many young people pursuing these occupations

Who’s Driving? SAE Automation Levels

SECTION 1: VOLUNTARY GUIDANCE

SAE AUTOMATION LEVELS

Full Automation

0	1	2	3	4	5
No Automation	Driver Assistance	Partial Automation	Conditional Automation	High Automation	Full Automation
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Who's Driving? Drivers and vehicles-no easy answers

- **Drivers: Language in draft Congressional legislation specifically prohibits states from requiring a driver license for use of level 4 and 5 vehicles**

- **For levels 3 and under, DMV would continue to test/issue driver licenses**

- **Will level 3 vehicles require an endorsement on the driver license to ensure driver is knowledgeable about operation of such a vehicle?**

- **Will mandatory training be required for purchasers of automated vehicles, through driver education, manufacturers, or dealers?**

Who's Driving? Vehicle Registration

- **Should manufacturers be required to advise the customer and DMV of level of automation on a given vehicle?**
- **Should it be noted on the registration, making it available to law enforcement, insurance companies, owners?**
- **How are policy makers guaranteed that owners/drivers are aware of the vehicle's autonomy and how to use it safely?**
- **How to ensure law enforcement knows how to: address an AV involved in a crash; disengage the driving system; collect information about the crash, and the information recorded prior to the crash?**

Who's Driving? Liability Issues to be resolved

- Who must carry and possess proof of liability insurance?

- Many opinions insist that it will depend on who is driving; is the human or the automated driving system in control?

- Does control define the driver (human or system) of the vehicle?

- If the system is in control, who carries liability insurance; the owner, the driver or occupant, or the technology provider?

Who's Driving? Challenges ahead

- **Articles on AVs and CVs are published daily**

- **There are many contributors trying to formulate the ideal method for programming and deployment**

- **The challenge is to ensure safe roads, safe vehicles, and safe drivers: while incorporating AV technology into laws and regulations in a way that promotes industry, commerce, and safety**

- **Determinations of what is right for Idaho and its citizens, while ensuring uniformity with other jurisdictions to promote interstate commerce.**

State of Connecticut's Efforts to write AV legislation

- **Recent AAA survey published:** https://tinyurl.com/yaz6rpwl

Questions?

Contact: Amy Smith
DMV Policy Analyst
208-334-8708
amy.smith@itd.idaho.gov

Idaho Autonomous Vehicle And Connected Vehicle

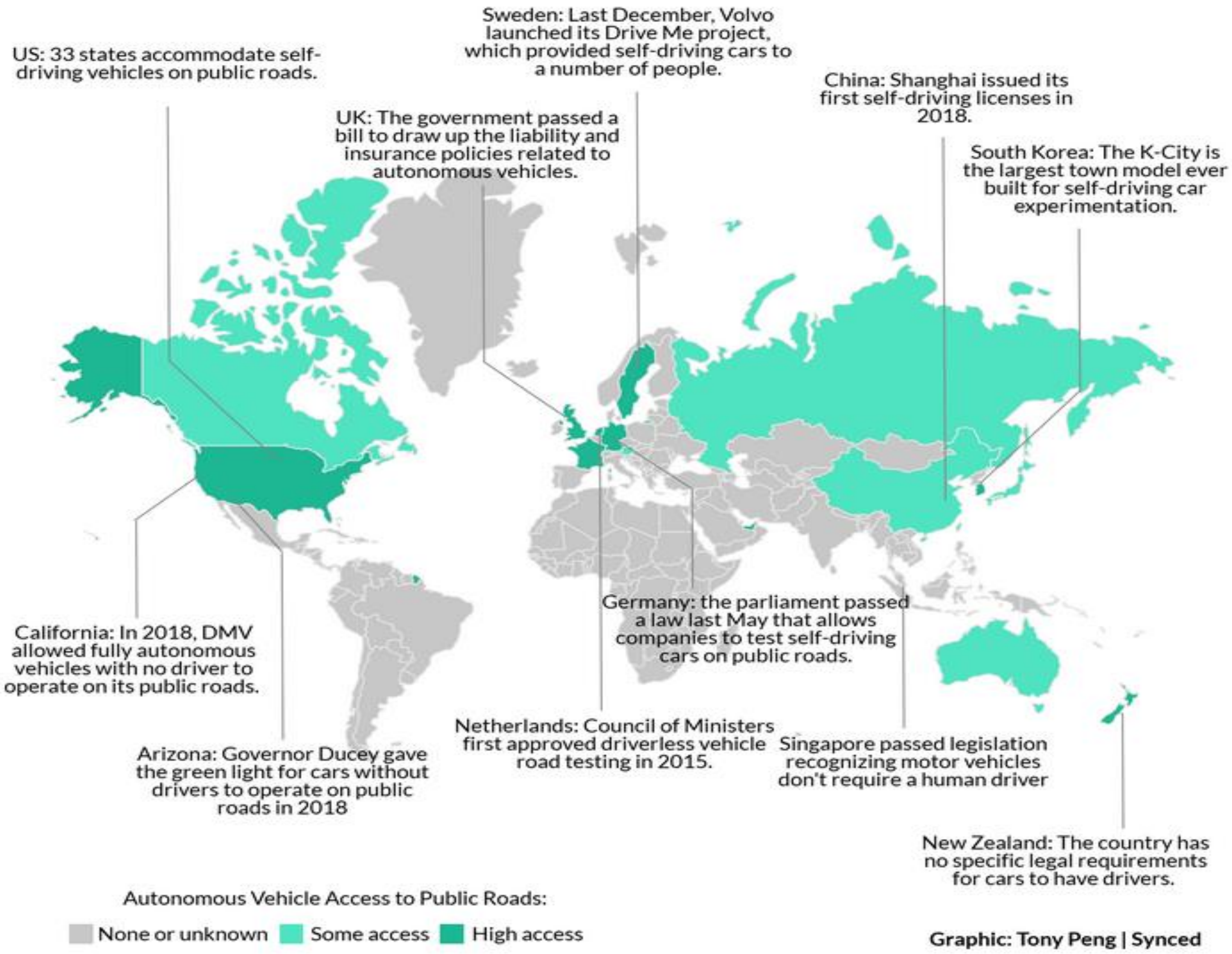
Testing and Deployment Committee

Testing and Certification

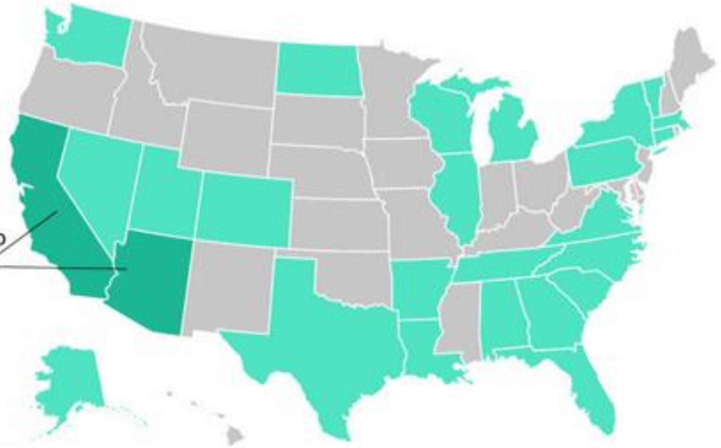
Dr. Ahmed Abdel-Rahim

University of Idaho

Autonomous Vehicle Testing – Global Overview



Autonomous Vehicle Testing – Global Overview



Autonomous Vehicle Testing and Certification: Legal Framework

To provide for safe testing of autonomous vehicles, three different legal "instruments" are being used :

- **Binding regulation**
  - California (Division 16.6, Section 38750 of the California Vehicle Code)
- **Non-binding regulation**
  - The U.S. Federal Government: (USDOT/NHTSA Federal Automated Vehicles Policy)
  - The U.K.: Department for Transport Code of Practice to provide guidance for anyone wanting to conduct testing of(highly) automated vehicles on public roads.
- **Granting exemptions**
  - The Netherlands: the Dutch Vehicle Authority (RDW) has been given the competence to grant exemptions from certain laws if these exemptions are useful for the testing of automated vehicle functions.

February 2018 final version of the California regulations.

The California autonomous vehicle testing program has now four clear requirements that manufacturers must meet:

- The testing can be done only by the manufacturer;
- The testing can be conducted only by a licensed driver or remote controller hired by the manufacturer;
- The manufacturer must provide financial proof of $5 million;
- The manufacturer must present either a general or a driverless testing permit.

- The 2018 regulations are different from what the state had taken back in 2015. Back then, it was seeking a more restrictive approach towards autonomous vehicles, but its approach has now changed!

Safe Testing of Highly Automated Vehicles

A successful path must include:

- Appropriate government oversight
  - developed in coordination with strong stakeholder engagement formed through partnerships with the many entities <u>engaged in</u> or <u>affected by</u> these rapidly developing technologies.

- Effective partnerships
  - should include representatives from broad reaching government organizations, government support associations, industry, research institutes, and advocacy groups.

Safe Testing of Highly Automated Vehicles

American Association of Motor Vehicle Administrators: Jurisdictional Guidelines:

- Administrative Considerations;
- Vehicle Credentialing Considerations;
- Driver Licensing Considerations; and
- Law Enforcement Considerations.

Other issues to be considered:

- commercial motor vehicles operations, training and workforce development for agency staff, jurisdictional safety inspection programs and criteria, data privacy and security, cybersecurity, and enabling infrastructure,

Idaho Autonomous Vehicle And Connected Vehicle Testing and Deployment Committee

Testing and Certification Discussion

Dr. Ahmed Abdel-Rahim
University of Idaho

Idaho Autonomous Vehicle And Connected Vehicle Testing and Deployment Committee

Safety

John Tomlinson
Idaho Transportation Department

Idaho Autonomous Vehicle And Connected Vehicle Testing and Deployment Committee

Safety Issues: What States Can Do

SAFETY FACTS

the House.

TO POST ROADS

The Idaho Department of Highways reminded truckers Friday that it will begin posting some roads for reduced speed and load limits about the first of February, because of spring break-up in roads due to thawing.

IDAHO TRAFFIC DEATHS

1959 total to date....... 8
1958 total to date....... 7
1957 total to date....... 9

Idaho Statesman

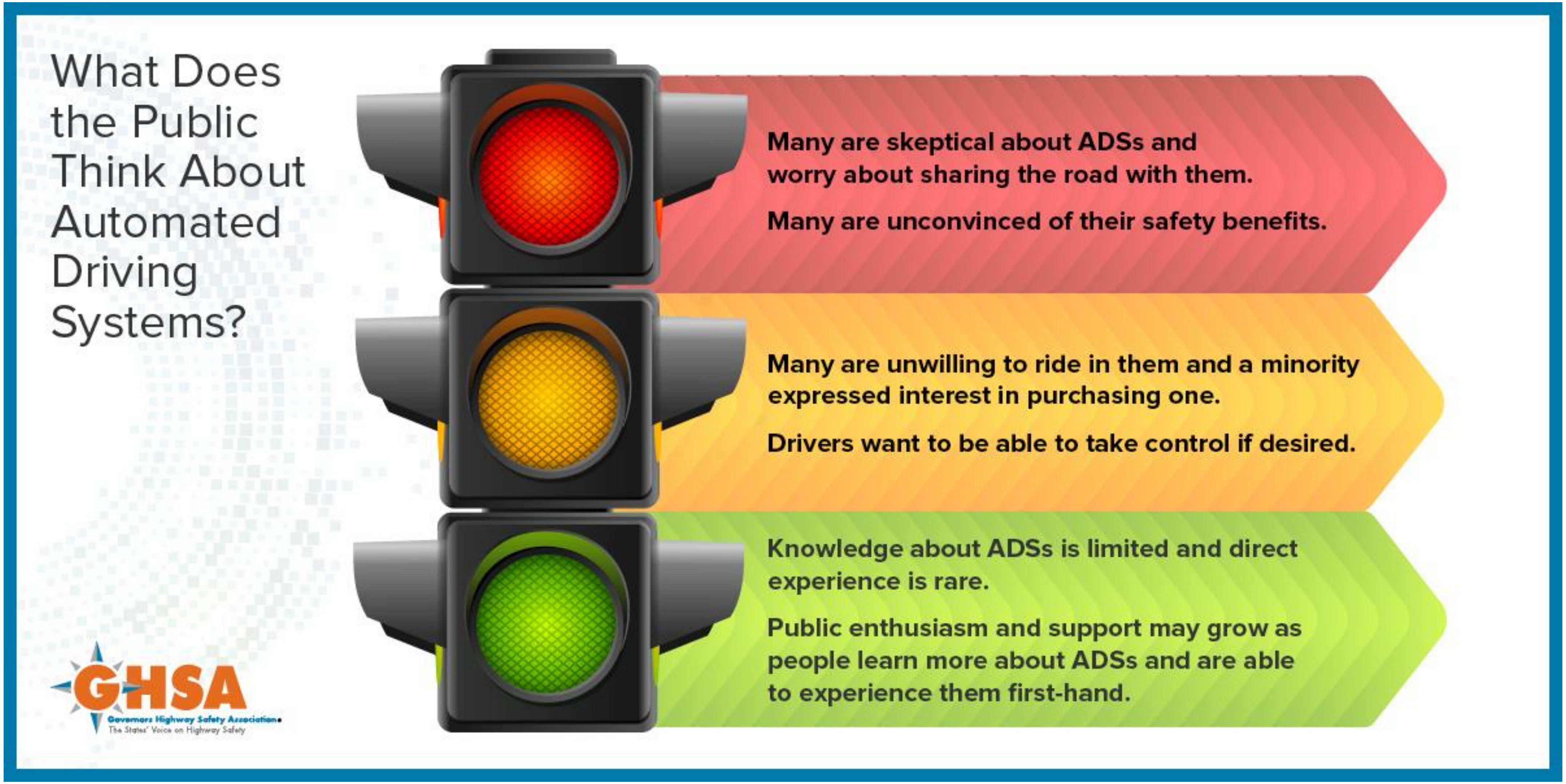
January 24, 1959

37, 461

253

244

PUBLIC OPINIONS



ELEMENTS OF SAFETY

SYSTEM SAFETY	OPERATIONAL DESIGN DOMAIN	OBJECT AND EVENT DETECTION AND RESPONSE	FALLBACK (MINIMAL RISK CONDITION)
VALIDATION METHODS	HUMAN MACHINE INTERFACE	VEHICLE CYBERSECURITY	CRASHWORTHINESS
POST-CRASH BEHAVIOR	DATA RECORDING	CONSUMER EDUCATION AND TRAINING	FEDERAL, STATE AND LOCAL LAWS

BEHAVIORAL SAFETY ISSUES

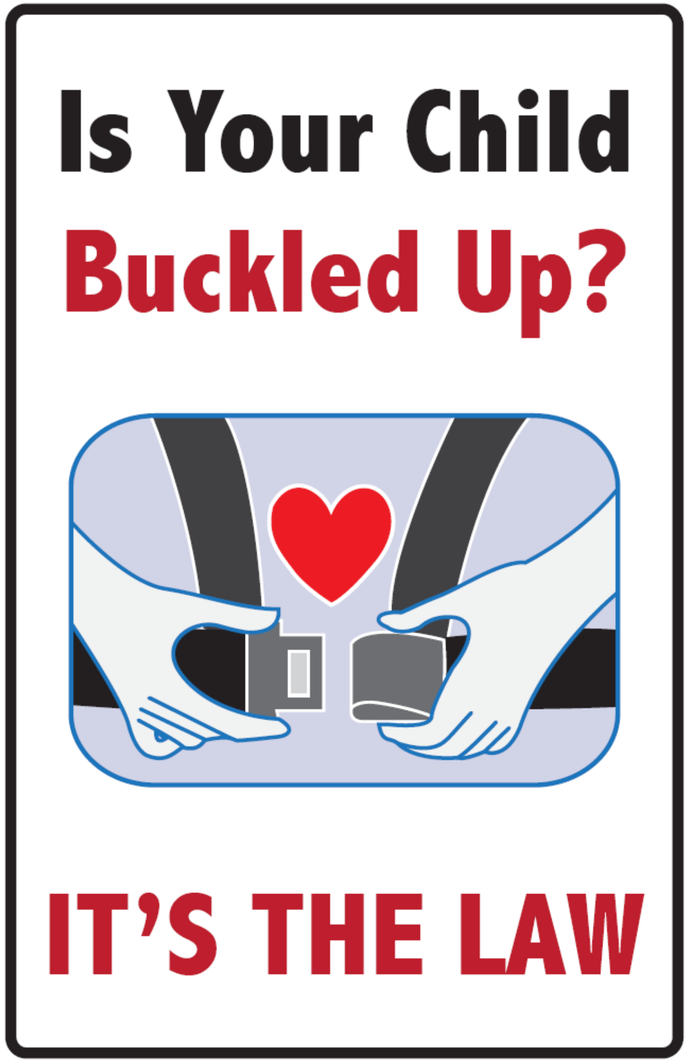
Traffic Laws and Flows

Decision Making

Recognition and Reaction

System Failure

SAFETY ISSUES



Belts and Laws

Child Restraints

Communication

Law Enforcement

RECOMMENDATIONS FOR STATES

Traffic Law Changes

Educate the Public

Work with Law Enforcement

Work with DMV

EDUCATING THE PUBLIC

LAW ENFORCEMENT

Idaho Autonomous Vehicle And Connected Vehicle Testing and Deployment Committee

Safety Discussion

John Tomlinson
Idaho Transportation Department

Idaho Autonomous Vehicle And Connected Vehicle Testing and Deployment Committee

Wrap-Up

Brian Ness
Director, Idaho Transportation Department

Idaho Autonomous Vehicle And Connected Vehicle Testing and Deployment Committee

Adjourned