VIRGINIA
IT AGENCY

Information Security Officer's Advisory Group

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Wesley Dupree/VITA
2025 Server operating system (OS) refresh	John Del Grosso/VITA
Virginia Identity (VID)	Franklin Thurston/VITA
Securing the Transition: Navigating Risk During a Gubernatorial Shift	Mike Watson/VITA
Securing the Future of Mobility: Cybersecurity Challenges and Research at the Center for Transportation Research	Kevin Heaslip/University of Tennessee
Upcoming Events	Wesley Dupree/VITA
Adjourn	

VIRGINIA
IT AGENCY

2025 Server operating system (OS) refresh

John C. Del Grosso

Aug. 6, 2025

Discussion today

- Refresh project initiation
- VITA Enterprise Architecture Roadmap & MS Support Durations
- OS population
- Support Model Timelines
- Types of OS upgrades
- General guidelines
- OEM operating system support
- Upgrade thoughts

Refresh project initiation

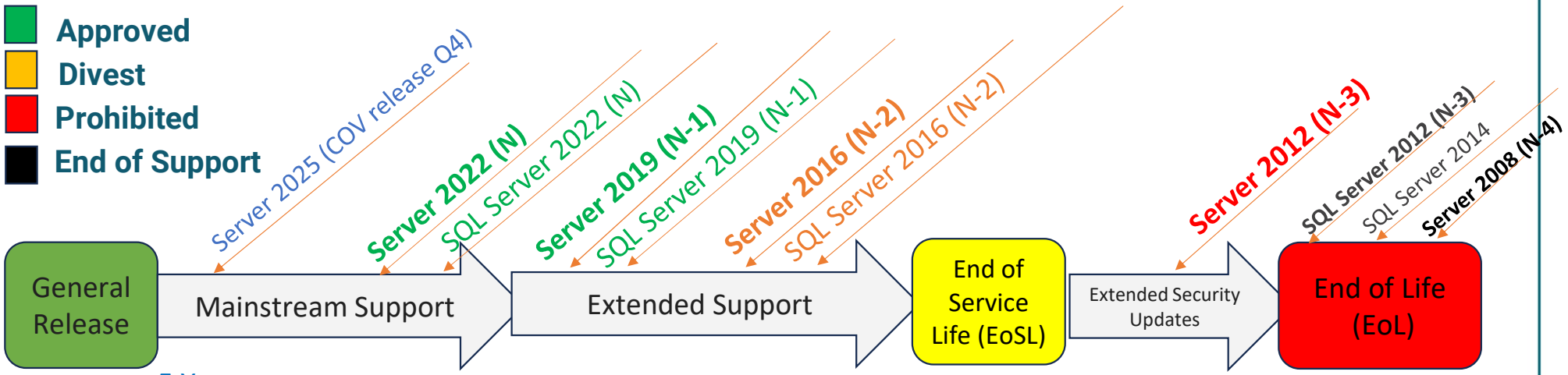
Overview of initiation mechanisms

- **Annual refresh currency project (ARCP):** All activities are coordinated through the ARCP project manager for all facets of OS and structured query language (SQL) upgrade.
- **Request for solution (RFS):** The upgrades are initiated by an agency submitted RFS: general requirements form.
  - List the servers on the RFS form with a notional schedule and upgrade order.
  - In many cases, this will be a 'no-cost' demand – depending on the agency needs.
  - If there are additional services requested beyond the OS upgrade, they may require billing.
  - N-1 to N upgrades (e.g. OS 2019 to 2022)

Upgrades by environment

- **Servers managed by Unisys will be upgraded via the ARCP:**
  - Commonwealth of Virginia (COV) data centers (agency and VITA)
  - Oracle cloud infrastructure (OCI)
  - Amazon web services (AWS)
- **Servers managed by NTT Data will require an agency-initiated demand record/ RFS:**
  - Microsoft Azure

VITA Enterprise Architecture Roadmap & MS Support Durations



5 Years
- Security patching- all
- Enhancements
- Features Updates
- Enhanced Support
- Warranty Support

5 Years
- Security patching - all
- Enhancements
- Enhanced Support
- KBA updates

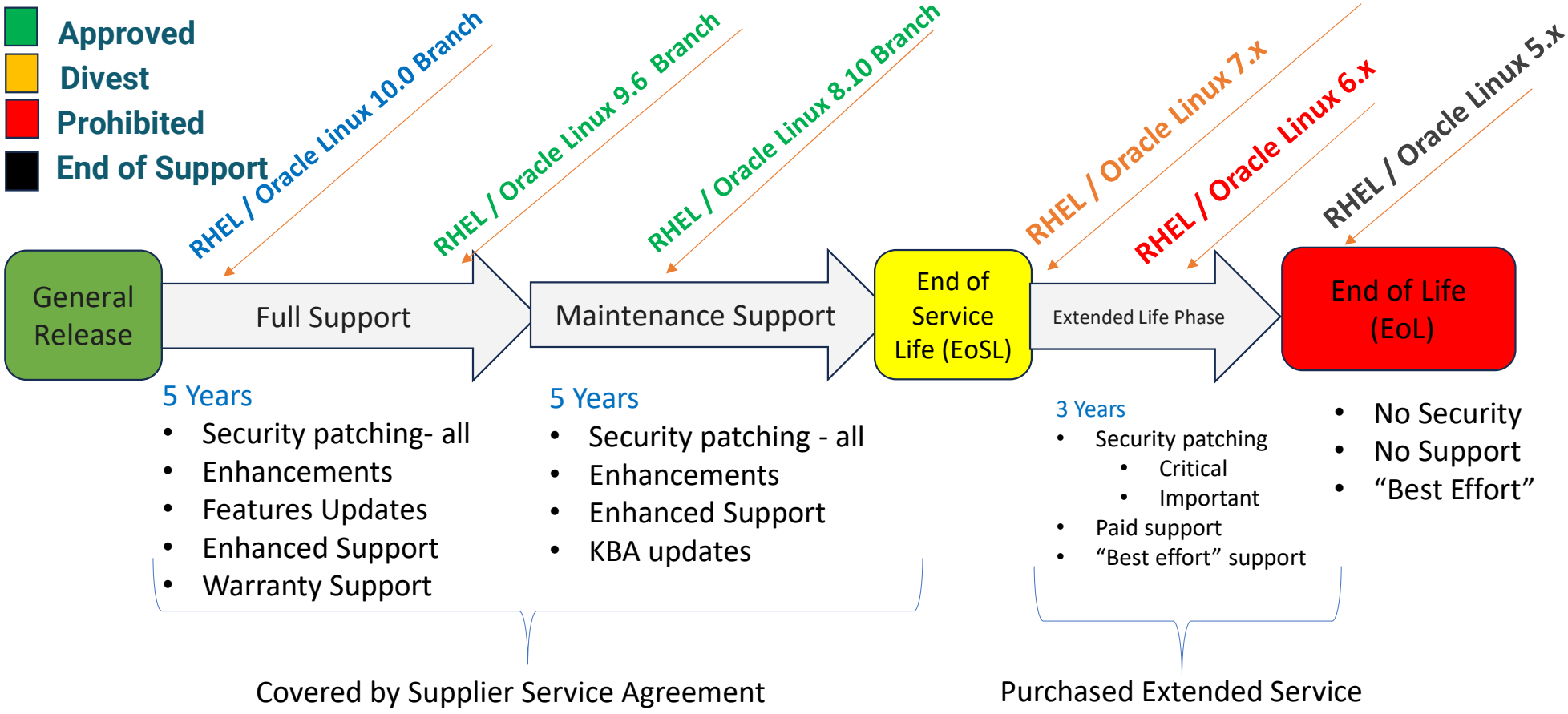
3 Years
- Security patching
  - Critical
  - Informational
- Paid support
- "Best effort" support

- No Security
- No Support
- "Best Effort"

Covered by VITA MSFT Enterprise Agreement

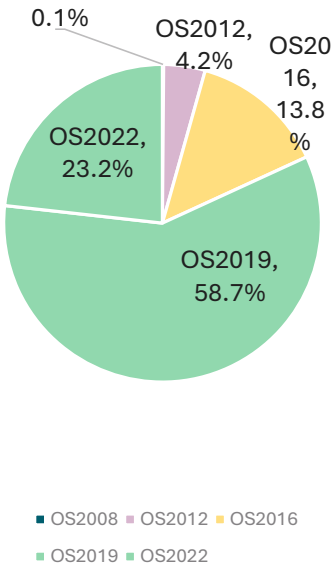
Purchased ESU Licensing

VITA Enterprise Architecture Roadmap & Linux Support Durations

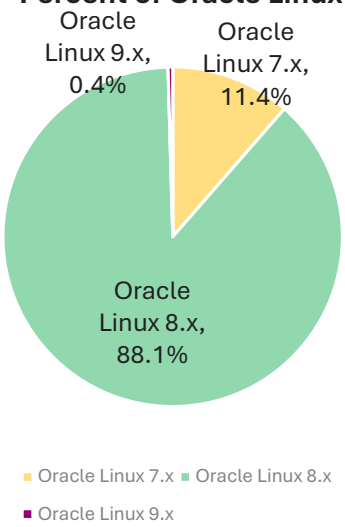


Operating system population (July 2025)

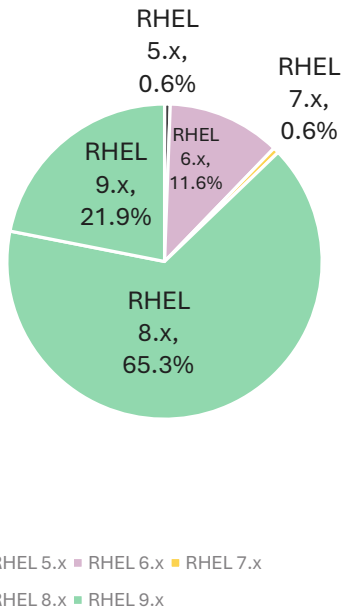
Percent of MS Server



Percent of Oracle Linux

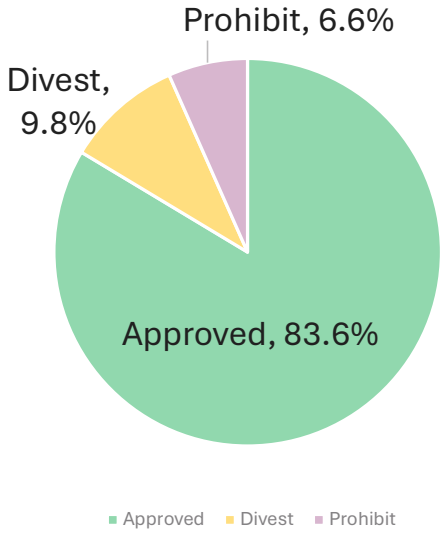


Percent of Red Hat Enterprise Linux



Aggregate

Percentage by Class



Approved: N & N-1

DIVEST: N-2

PROHIBITED: N-3+

Types of OS Upgrades

In-place: The existing server is upgraded to a new version.

- **Duration:** Typically, 4-6 hours, depending on complexity and patching updates needed.
- **Testing:** The agency should provide testers and server owner to be available during the in-place upgrade period.
- In-place upgrade should be discussed with the server's supplier first.
- In-place upgrades may result in remnants of the older OS version and existing Agency apps remaining, carrying forward existing vulnerabilities

Server migration: The current server with an outdated OS is replaced with a new server.

- **Agency request:** A new server should be ordered through the catalog. During migration, the agency will have two servers in billing (original and new) until a decommission request is initiated.
- A server migration is advised if:
  - Existing security vulnerabilities cannot be resolved due to end-of-life apps or non-supported app or tool versions
  - The server cannot be upgraded by in-place means. Most likely if upgrading 3 or more versions.
  - A physical server is end-of-support or end-of-life

General guidelines

- Upgrades offered to N-1 (OS2019, RHEL/OL8) or preferred, N (OS2022, RHEL/OL9) only.
- Upgrades from N-1 to N require an RFS at agency cost. From N-2+ are no-cost.
- Servers, in general, cannot be in-place upgraded more than 3 versions from existing
- Decommission requests must be initiated by the Agency (for Migration upgrades)
- Upgrades can be scheduled at any time of day or night and weekends.
- A server 'snap-shot' is taken before every upgrade to allow for immediate roll-back
- Enterprise Architecture (EA) exceptions are required for servers remaining in "Divest" and "Prohibited" status for servers with support (e.g. Windows OS2012/16, Linux/OL7)
- Security exceptions (SEC EXC) are required for servers in "Divest" and "Prohibited" status for servers in N-2+ that are without support (e.g. Windows OS2008, RHEL7/OL6 and below)

Upgrade parting thoughts

Upgrade-fatigue is a real thing. Plan your upgrades at a cadence that keeps you at N and N-1 continuously – every three years to avoid fatigue. Always upgrade to N.

The technology roadmap and OS version drive "N"-level - not the support profile.

Keep your Agency applications up-to-date, make sure they are forward compatible and supported with future OS versions – consider SaaS and Public Cloud offerings.

Completely remove old versions of apps and tools as they leave remnants that get flagged in Tenable as vulnerabilities.

Extended support: not always offered by the OEM. Not announced until one year from EoSL.

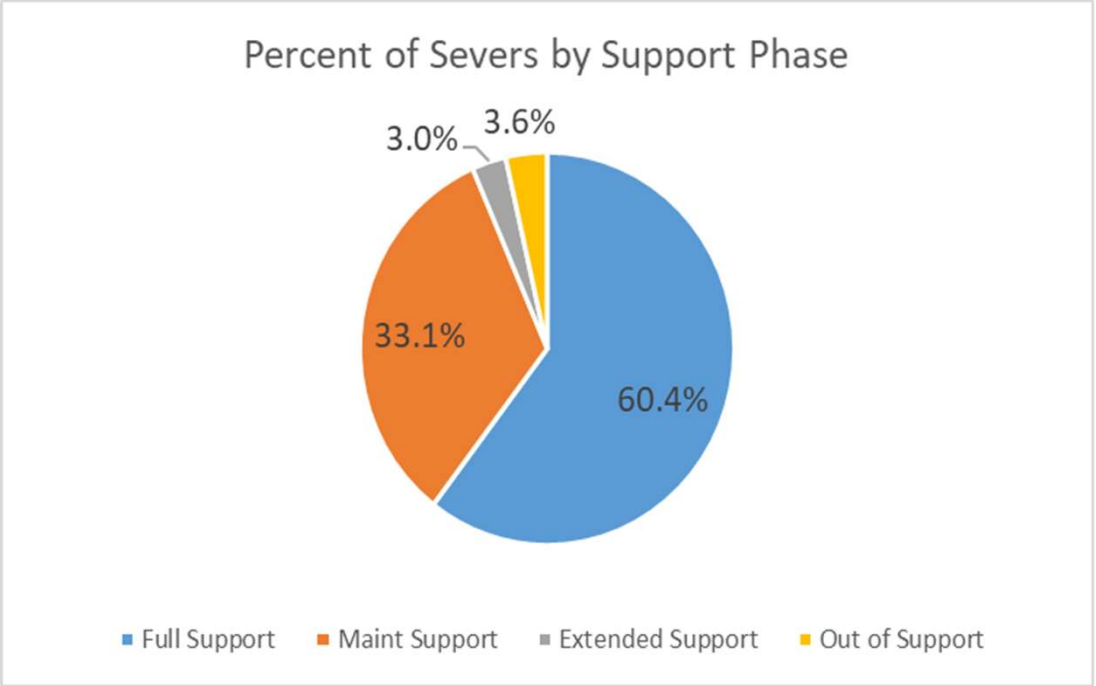
Future restrictions on N-2+ versions are in planning to drive upgrade participation.

Population of Servers by OEM OS Support Phase

93.5%

of COV servers operating systems are fully supported as provided by the OEM (Microsoft/RHEL/Oracle Linux).

- ✓ Full Security Support
- ✓ Enhancements
- ✓ Enhanced Support



Questions?

VIRGINIA IT AGENCY

Virginian Identity (VID)

Partner persona

Franklin Thurston

Aug. 6, 2025

SPLM process to extend VID to the partner persona

VID current state:

- Provides a single sign-on (SSO) service for COV applications
- Based on the Okta Customer Identity and Access Management (CIAM) SSO solution that has been implemented in a FedRAMP High tenant
- Applications eligible to join the VID SSO service serve the public user persona
- Working through the SPLM process to extend VID to the partner persona

Increased scope with the partner persona:

- Applications eligible to join the VID SSO service serve the public user and partner persona
- Adding additional multi-factor authenticators (MFA) for business partners

Current scenario for the enterprise

- Agency silos force citizens to navigate multiple login systems, repeatedly provide the same sensitive information, and manage separate accounts and credentials for different services causing identity sprawl
- Legacy systems that are incapable of supporting secure, rapid information sharing within and across agencies impose additional burdens on applicants
- Weak password systems create security gaps inviting breaches and fraud
- Legacy systems, especially those with outdated identity controls leave agencies increasingly vulnerable

Agency challenges

- Budget: Escalating cybersecurity threats and demand for better digital experiences create mounting budget pressures
- Agency IT executives often must prioritize core functions like the mounting costs to maintain legacy systems over much needed upgrades and innovation
- It is estimated that some agencies spend up to 80% of their budgets to maintain outdated systems that don’t meet today’s needs and demands
- Skills gap: As experience staff reach retirement or leave, legacy knowledge leaves the agency creating the burden of maintaining legacy systems with diminishing expertise

Benefits of Virginian Identity

- Unification of citizen access and identity governance through centralized management
- Secure frictionless authentication across digital services
- Strengthens security controls
- Adaptive MFA based on risk level
- Automated compliance monitoring and reporting
- Eliminates silos and automates access management across systems
- Improved citizen experience through one SSO
- Built-in controls and automated enforcement streamline compliance
- Cost savings for agencies and enterprise

Pertinent VID links

- VID service catalog request form
- VID FAQs
- VID overview and benefits
- VID cost structure
- VID billing training video
- VID glossary
- Identity access management – separation of tenants

Questions?

Thank you for attending

vi_help@vita.virginia.gov

VIRGINIA
IT AGENCY

Securing the Transition: Navigating Risk During a Gubernatorial Shift

Michael Watson – Chief Information Security Officer of the Commonwealth, VITA Deputy CIO

August 6, 2025

How Risk Posture Changes During a Transition

- Leadership turnover delays decisions and approvals
- Cybersecurity policies and strategies face reevaluation
- Insider threats increase during staff and leadership transitions
- External threat actors exploit periods of political change
- IT and security budgets may be paused or reassessed

How ISOs Can Account for Elevated Risk

- Reassess agency-specific cyber risks and reprioritize controls
- Revalidate access controls, especially privileged users
- Update incident response plans and leadership contact lists
- Proactively brief new leadership on security posture
- Monitor for targeted threats (e.g., phishing, impersonation)
- Track any new executive orders or legislation

Practical Tools for ISO Transition Management

- Transition Cyber Risk Assessment Checklist
- Access Audit Tracker & Offboarding Logs
- IR Plan Contact Update Forms
- Leadership Cybersecurity Brief Template
- Threat Intelligence Alerts & SOC Monitoring

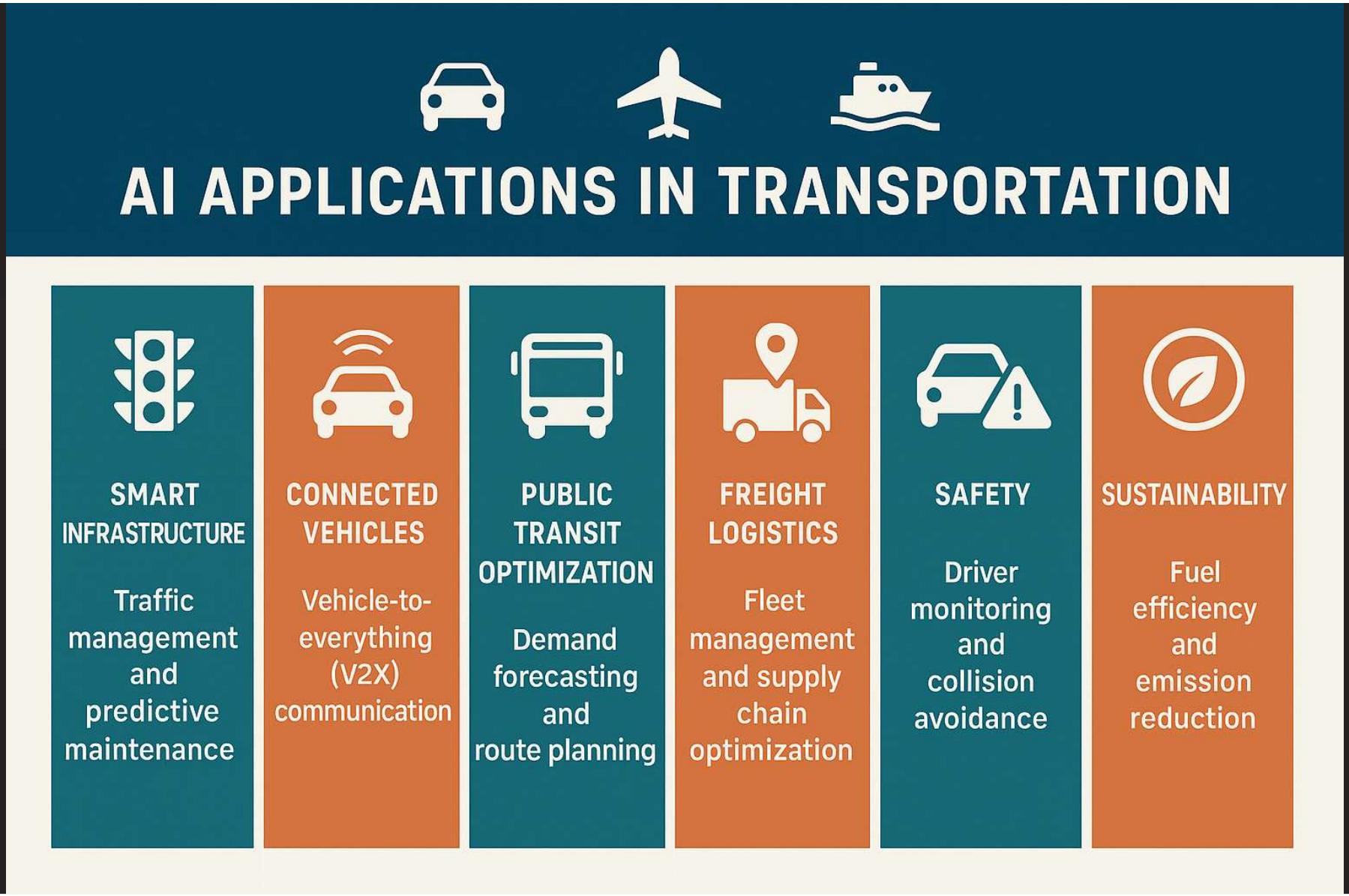
Summary of Key Risks and ISO Responses

- **Leadership Turnover → Update command and communication lines**
- **Insider Threat → Tighten access and offboarding procedures**
- **Policy Uncertainty → Continue compliance and advocate continuity**
- **External Threats → Watch for phishing, impersonation, deepfakes**
- **Budget Delays → Communicate funding risk impacts to new execs**

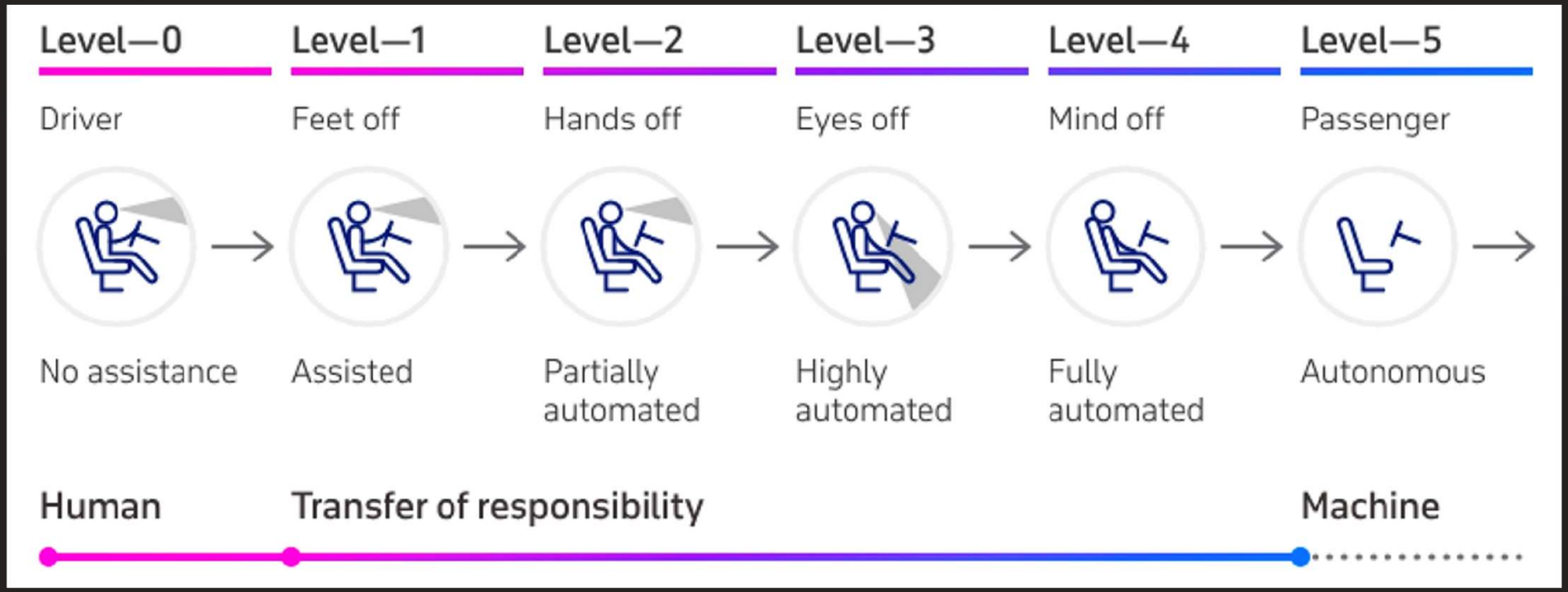
Questions?

Securing the Future of Mobility: Cybersecurity Challenges and Research at the Center for Transportation Research

Kevin Heaslip
Director, Center for Transportation Research


AI APPLICATIONS IN TRANSPORTATION
SMART INFRASTRUCTURE
Traffic management and predictive maintenance
CONNECTED VEHICLES
Vehicle-to-everything (V2X) communication
PUBLIC TRANSIT OPTIMIZATION
Demand forecasting and route planning
FREIGHT LOGISTICS
Fleet management and supply chain optimization
SAFETY
Driver monitoring and collision avoidance
SUSTAINABILITY
Fuel efficiency and emission reduction

Levels of Automation in Vehicles



Source: Appinventiv

How AI Enhances Advanced Driver-Assistance Systems

SENSORS

Camera

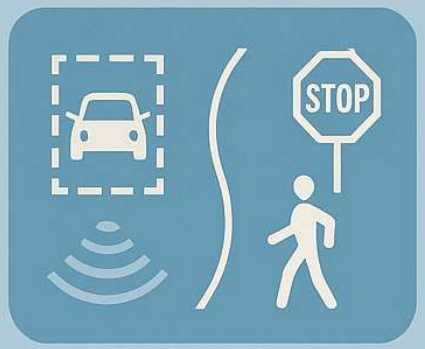
Radar

Ultrasonic Sensors

Ultrasonic Sensors

Ultrasonic Sensors

AI PERCEPTION



- Object Detection
- Lane Detection

ADAS FEATURES

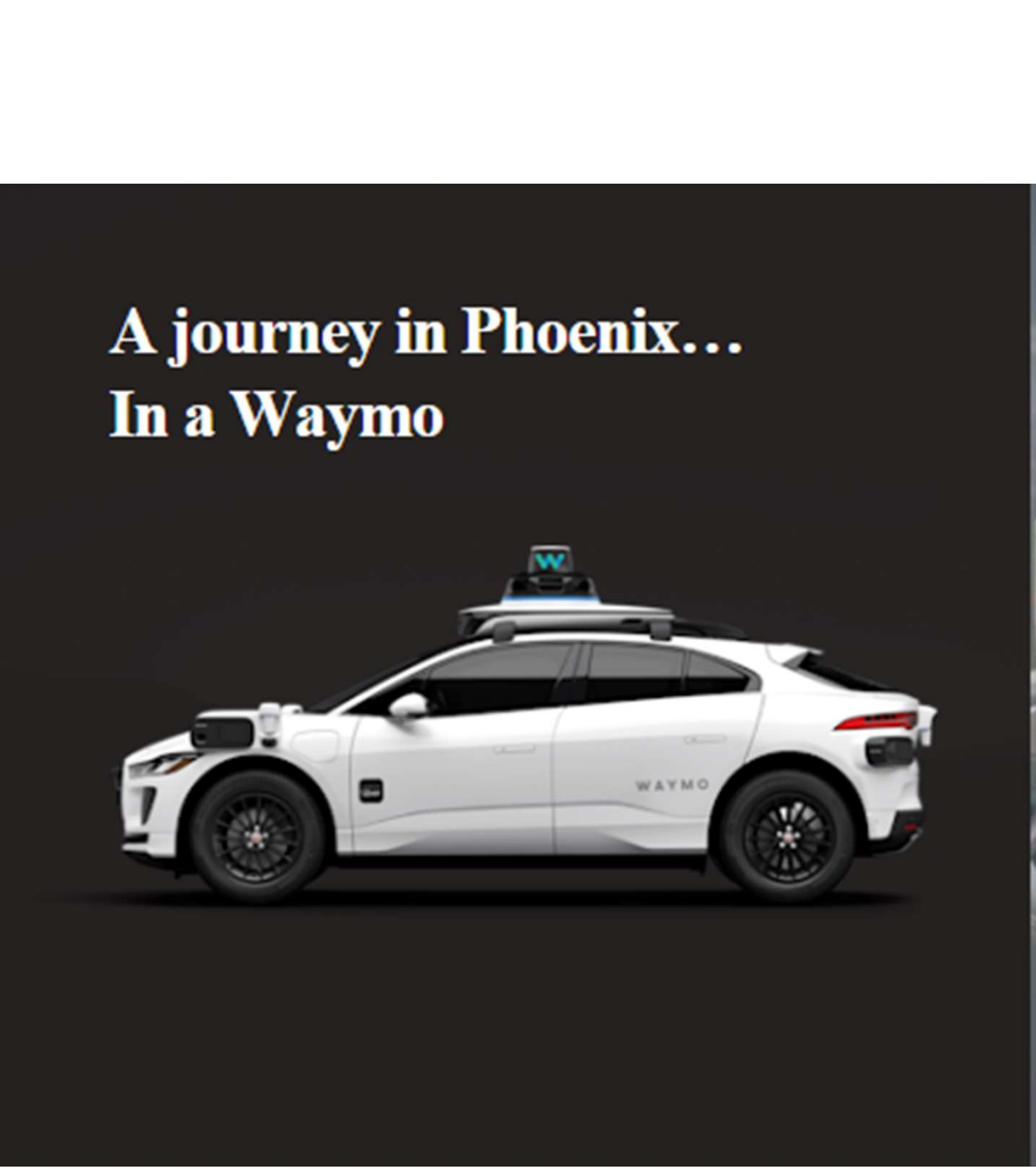
- Lane Keeping Assist
- Adaptive Cruise Control
- Automatic Emergency Braking
- Blind Spot Monitoring

BENEFITS

- Collision Avoidance
- Reduced Driver Fatigue

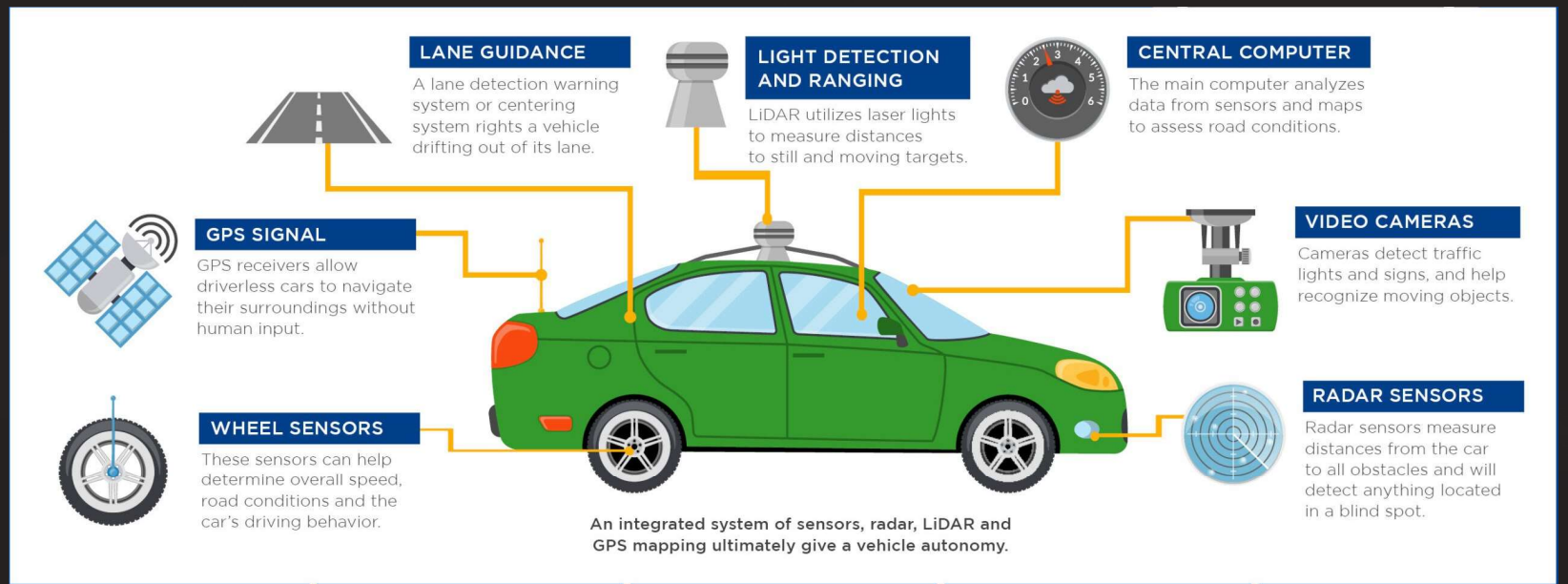
Our research vehicles

A journey in Phoenix…
In a Waymo

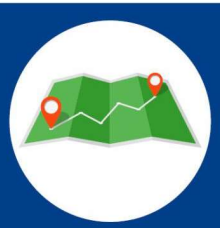


Another Waymo Ride...

Driverless Vehicle Components



An integrated system of sensors, radar, LiDAR and GPS mapping ultimately give a vehicle autonomy.



3D MAPS

Robust 3D maps are critical for identifying lanes, off-ramps and even curbs.

STEERING

Manufacturers are designing vehicles that won't require steering wheels.

GPS

While GPS helps determine location, one limitation is its reliance on a signal.

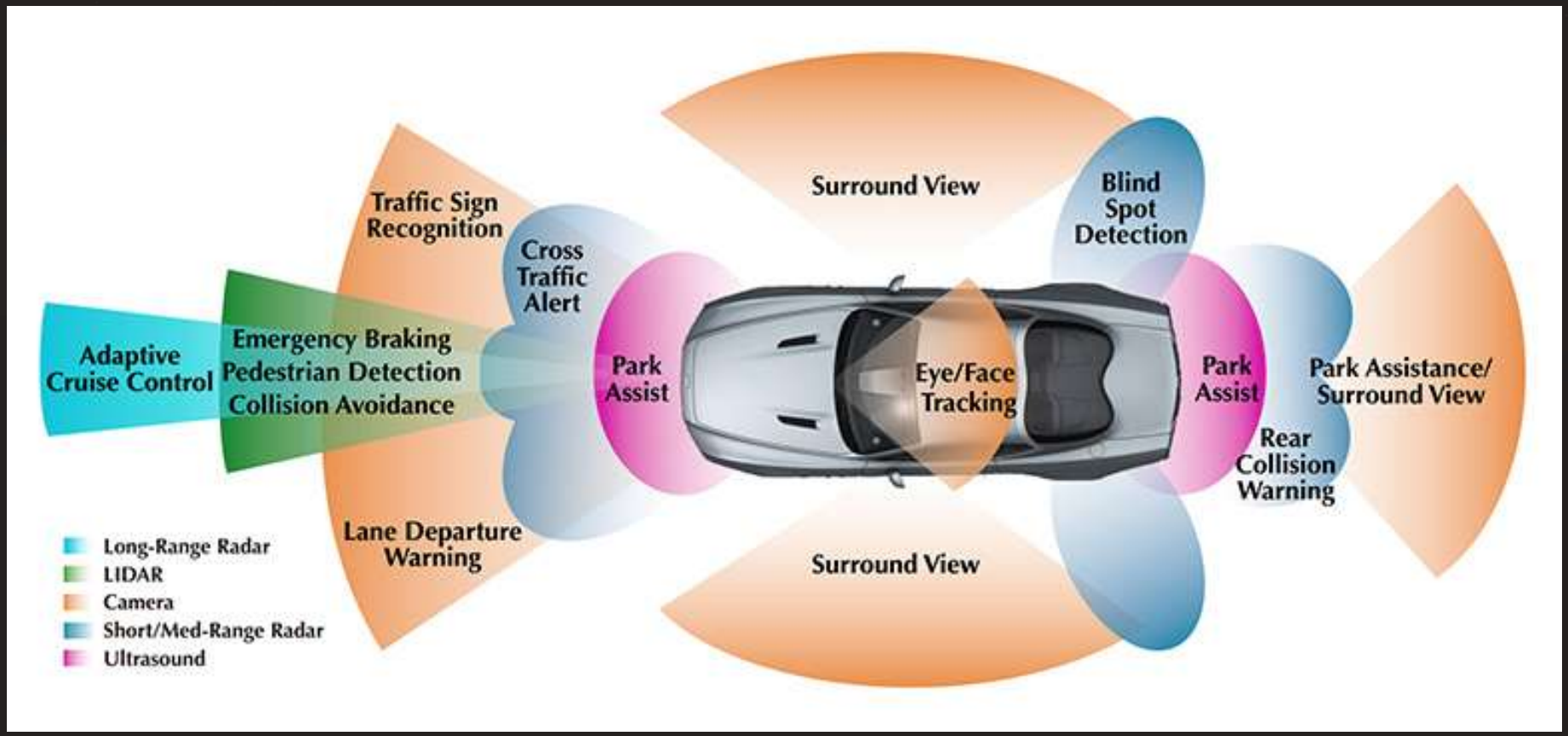
MAINTENANCE

Monitoring and maintenance will be critical, as sensory systems can fail.

HACKING

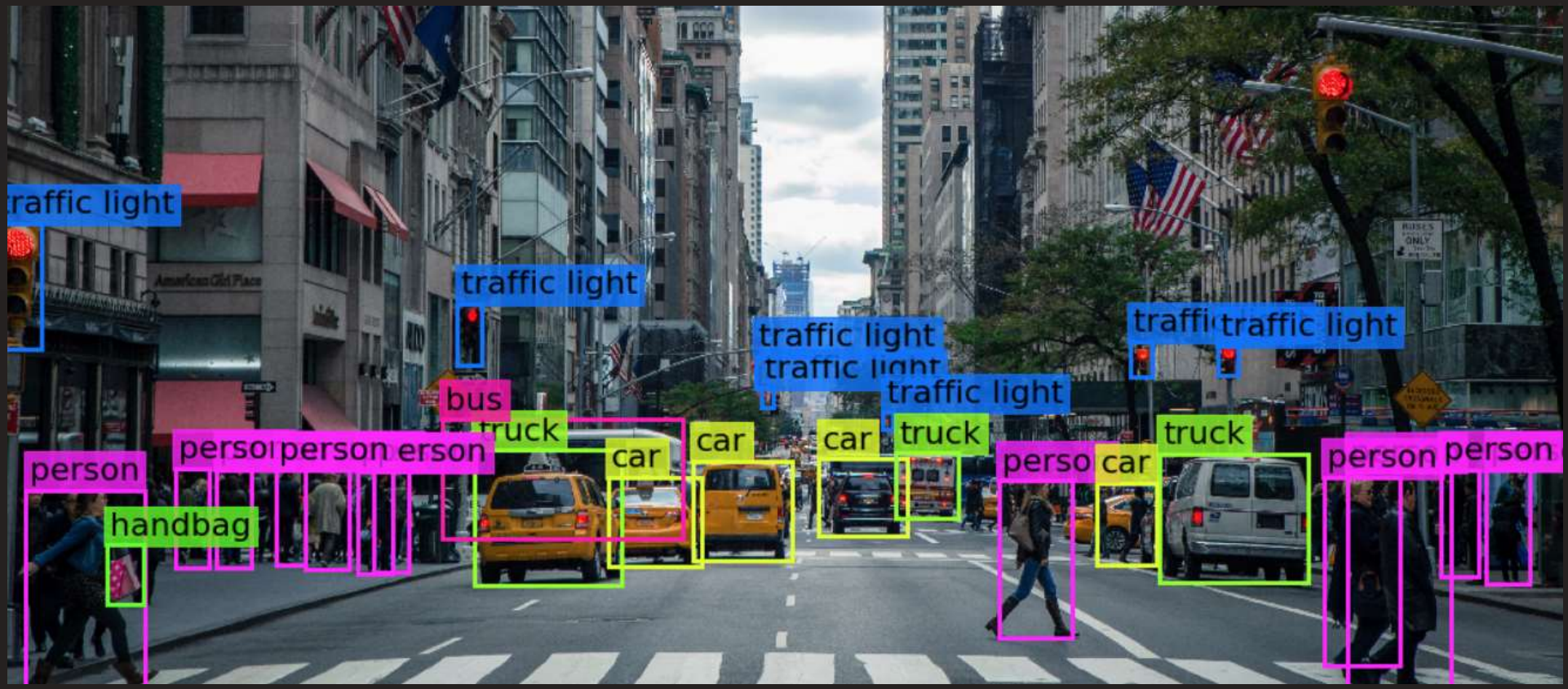
Self-driving car makers are paying special attention to security measures.

How vehicles sense the world



Source: Ecotron

Machine Vision

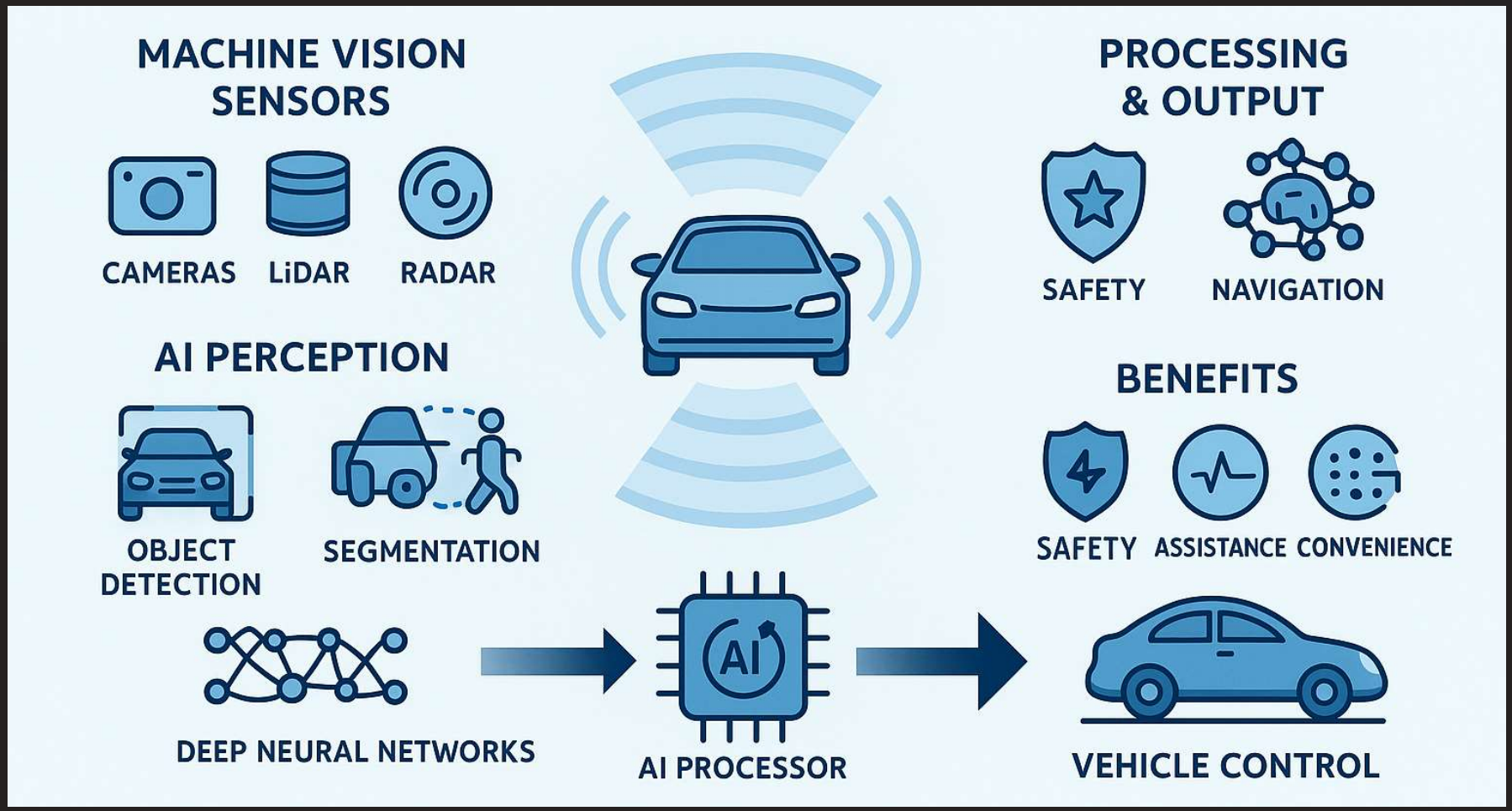


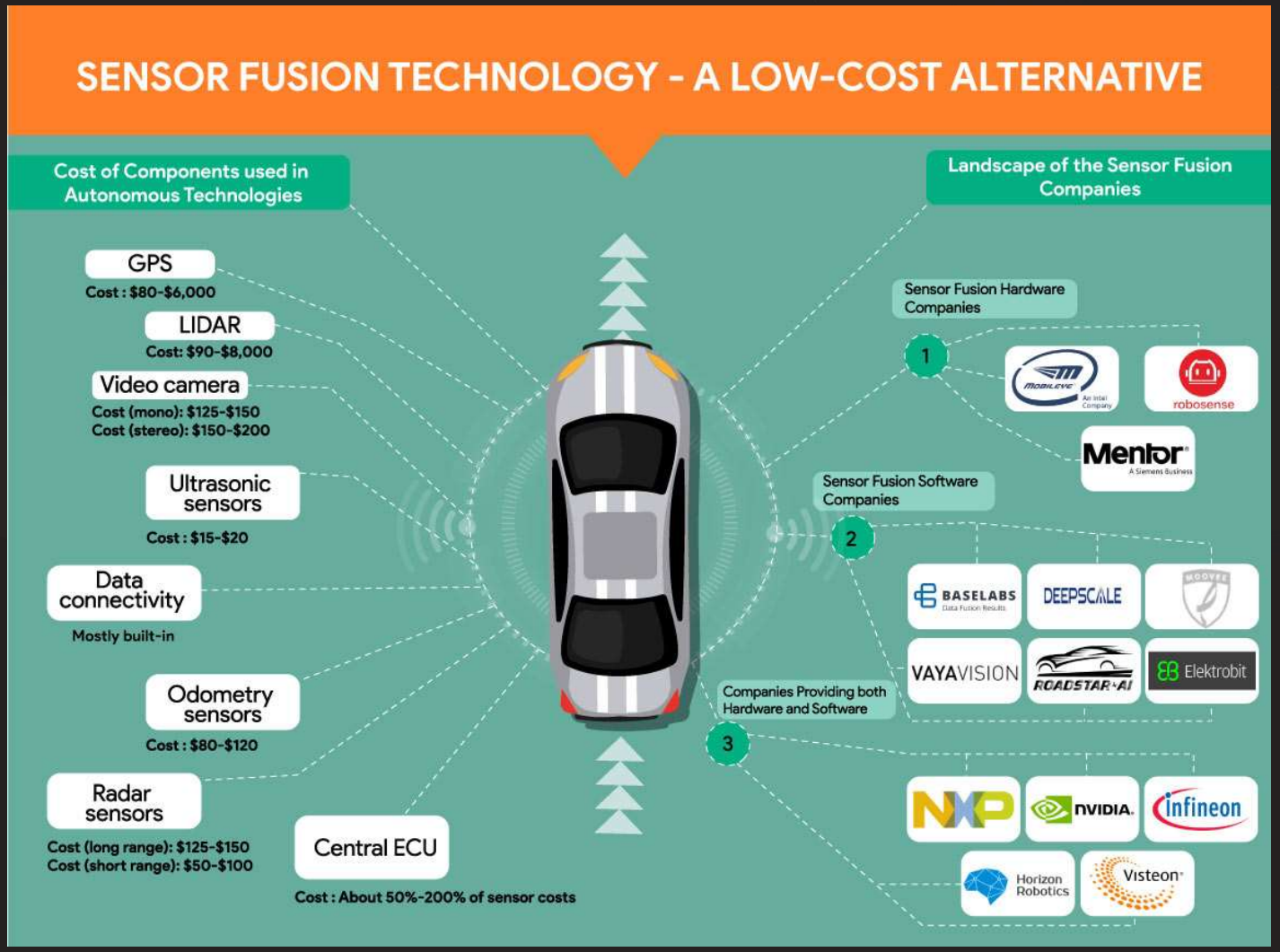
Source: Medium.com / Safwan Khan

LiDAR Real Time Mapping

Source: GPS World

Machine Vision and AI for Vehicles





Source: IdeaPoke AI

The Need for Sensor Fusion Technologies

Functional Features	LIDAR	Radar	Cameras	Ultrasonic	Multi-Sensor Fusion
Cost	High	Medium	Low	Low	Low
Object Detection	High	High	Medium	High	Very High
Object Classification	Medium	Low	High	Low	Very High
Pedestrian Detection	Medium	Medium	High	Low	Very High
Distance Estimation	High	High	Medium	High	Very High
Object Edge Precision	High	Low	High	High	Very High
Lane Tracking	Low	Low	High	Low	Very High
Range of Visibility	Medium	High	Low	Low	Very High
Distance – Accuracy	High	High	Medium	Low	Very High
Bad Weather Conditions	Medium	High	Low	High	Very High
Poor Light Conditions	High	High	Low	High	Very High
Velocity Calculation	Low	High	Medium	Low	Very High

Source: IdeaPoke AI

Cybersecurity

Protecting automotive electronic systems, systems, communication networks, control control algorithms, software, users, and and underlying data from malicious attacks, damage, unauthorized access, or access, or manipulation

Protect everything from a car's infotainment system to its wiring to the communication networks that run between its software and hardware

AI-powered data processors and chips

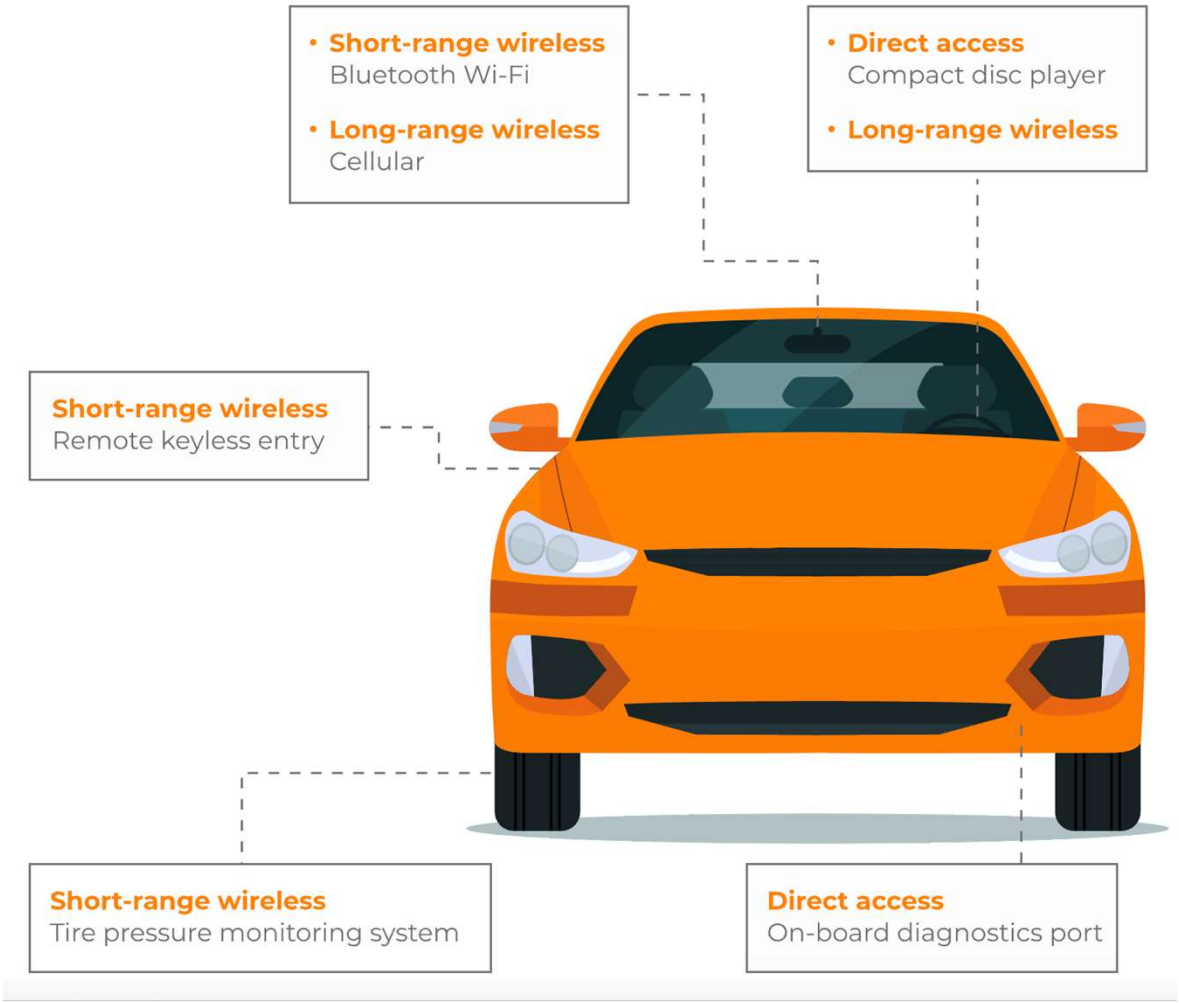
Electrical system engineering services for IoT hardware, software, devices, and vehicles

Cyber-physical systems (CPS)

Hardware security modules

NHTSA, Automotive Cybersecurity

Vehicle Attack Surfaces



Connected Vehicle Attacks

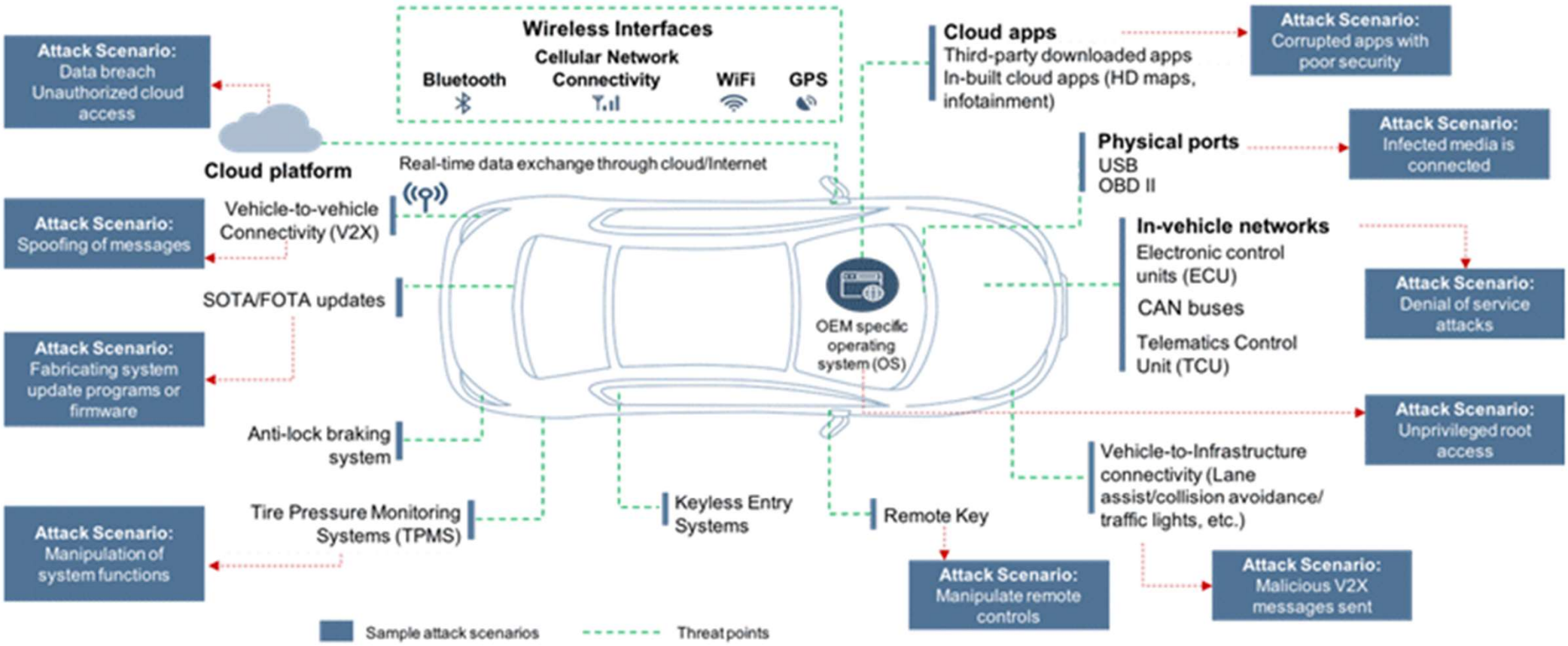


Figure 1: Potential Intrusion and Cyberattack Scenarios in Connected Vehicles

Source: Frost & Sullivan

Real-World Examples of Cyber Threats in Transportation

Jeep Cherokee Hack Incident

In 2015, researchers exploited vulnerabilities in the Jeep Cherokee's infotainment system, gaining remote control over critical vehicle functions, which led to a recall of over a million vehicles by Fiat Chrysler Automobiles to address these security flaws.

Real-World Examples of Cyber Attacks Affecting Vehicles

1

2015

The Jeep Cherokee hack demonstrated remote control vulnerabilities, leading to a major recall of 1.4 million vehicles.

2

2016

Hackers infiltrated a Tesla Model S, showcasing risks in wireless connectivity and prompting immediate software updates.

3

2020

Honda faced a ransomware attack that disrupted operations, highlighting potential vulnerabilities in connected vehicle systems.

4

2021

Significant vulnerabilities in China's connected vehicle networks affected over 220,000 vehicles, risking data manipulation.

5

2022

A data breach at Kia Motors and Hyundai raised concerns about the security of onboard systems linked to customer databases.

6

2023

Ongoing research continues to reveal new vulnerabilities in vehicle-to-everything (V2X) communications, threatening road safety.

Current Cybersecurity Measures in Vehicles

Proactive Threat Detection

Advanced Intrusion Detection Systems (IDS) utilize machine learning algorithms to analyze network traffic patterns, enabling real-time identification of potential threats and minimizing response times to cyber incidents.

Dynamic Firewall Adaptation

Modern firewalls in vehicles are equipped with adaptive capabilities that allow them to update security rules automatically in response to emerging threats, ensuring continuous protection against unauthorized access.

Regular Software Maintenance

Over-the-Air (OTA) updates not only enhance security but also improve vehicle functionality by providing manufacturers with the ability to deploy timely patches and feature enhancements, thereby maintaining optimal performance and safety.

Authentication and Encryption

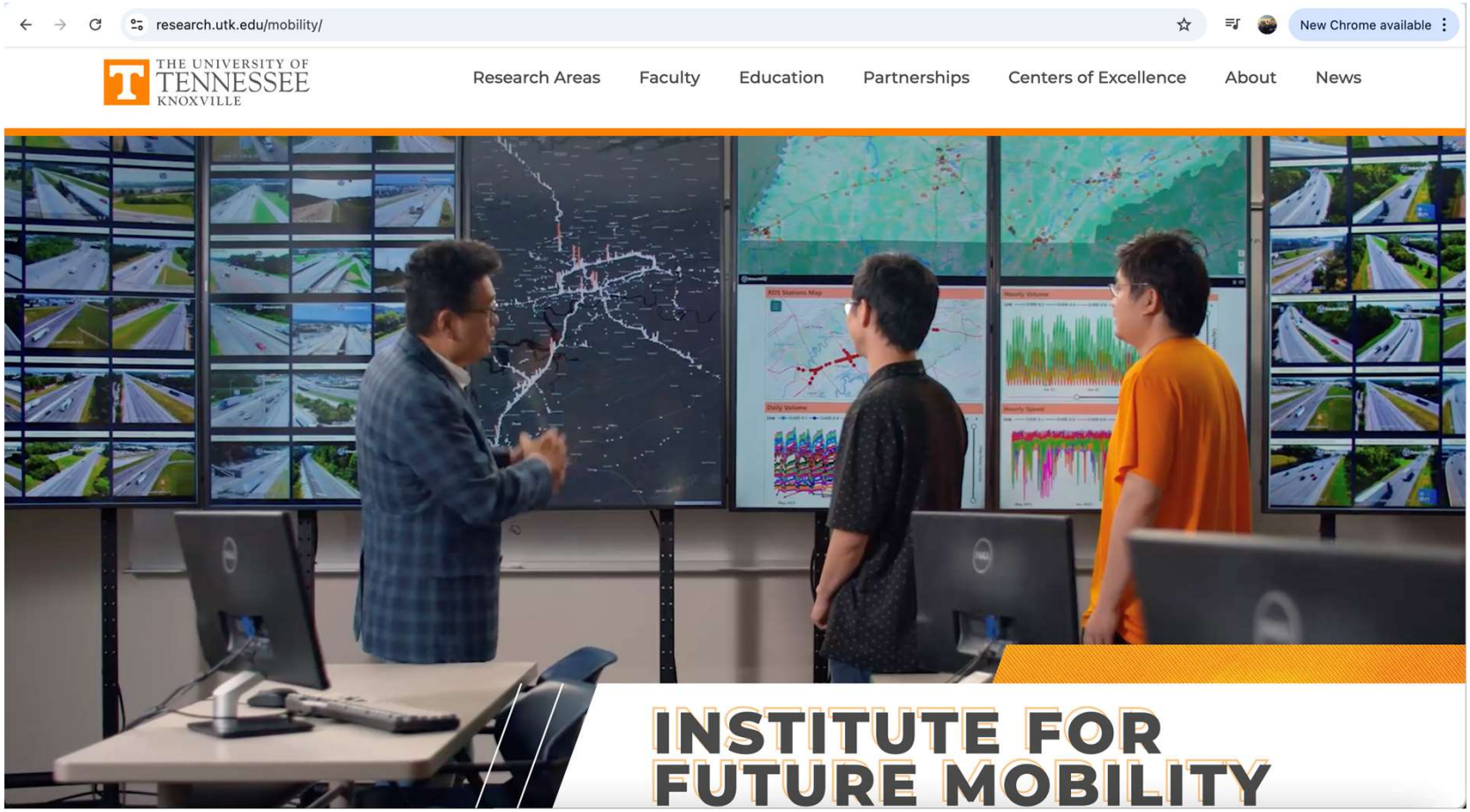
Importance of Robust Protocols

- **Implement robust authentication** protocols to confirm the identity of all parties involved in V2X communication.
- **Apply strong encryption methods** to protect data in transit between vehicles and infrastructure.
- **Maintain data integrity and confidentiality** to ensure messages cannot be tampered with or intercepted.
- **Prevent unauthorized access and cyber threats** that could disrupt V2X systems and jeopardize roadway safety.

Center for Transportation Research

1. CTR has been a nationally and internationally recognized research center at the University of Tennessee since 1972
2. CTR has over $13 million in programs under contract
3. CTR supports UT's responsibility to supply well-educated transportation students to the growing field of transportation professionals
4. CTR strives to address transportation research, education, and technology transfer needs for the nation, our region, and our community

Institute for Future Mobility



Future Mobility Research

DRIVING ECONOMIC GROWTH & JOB CREATION

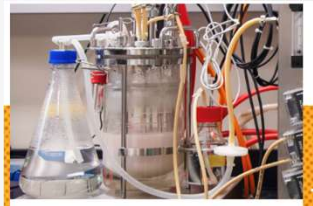
More than **900 companies** in the automotive manufacturing sector call our state home—and employ about **140,000 Tennesseans**. We are building on these strengths to ensure Tennessee leadership in the mobility sector for years to come.

LEADING ELECTRIC VEHICLE RESEARCH

Tennessee supports **40% of EV manufacturing jobs and investments** in the Southeast. UT is attracting new **industry investments in R&D** through partnerships with Tennessee-based OEMs like Volkswagen, Nissan, and Ford, as well as with industry leaders in energy storage, IT, and other strategic technology areas.

CATALYZING LOCAL & GLOBAL BENEFITS

The future of mobility affects everyone. UT research creates opportunities for a **safer, greener, and more secure mobility future** that enhances economic prosperity in Tennessee and around the world.

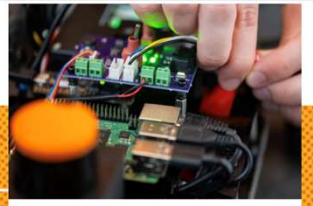


DECARBONIZATION

Investors, suppliers, and consumers are seeking sustainable transportation options. Our researchers are exploring two main strategies to this cleaner future: **alternative fuels** and **electrification**, including increasingly efficient power sources and charging strategies. We're pursuing cost-competitive solutions that improve vehicle performance, contribute to our nation's energy resilience, and shrink transportation's environmental footprint.

Learn about Alternative Fuels Research ····>

Learn about Electrification Research ····>



DIGITIZATION

There's a mobility revolution underway thanks to advances in **digital technologies**. Our research in **computational** and **communications tools** and systems puts Tennessee at the cutting edge. We're generating solutions that promise to move people and goods around the world more safely, efficiently, and effectively.

Learn about Digitization Research ····>

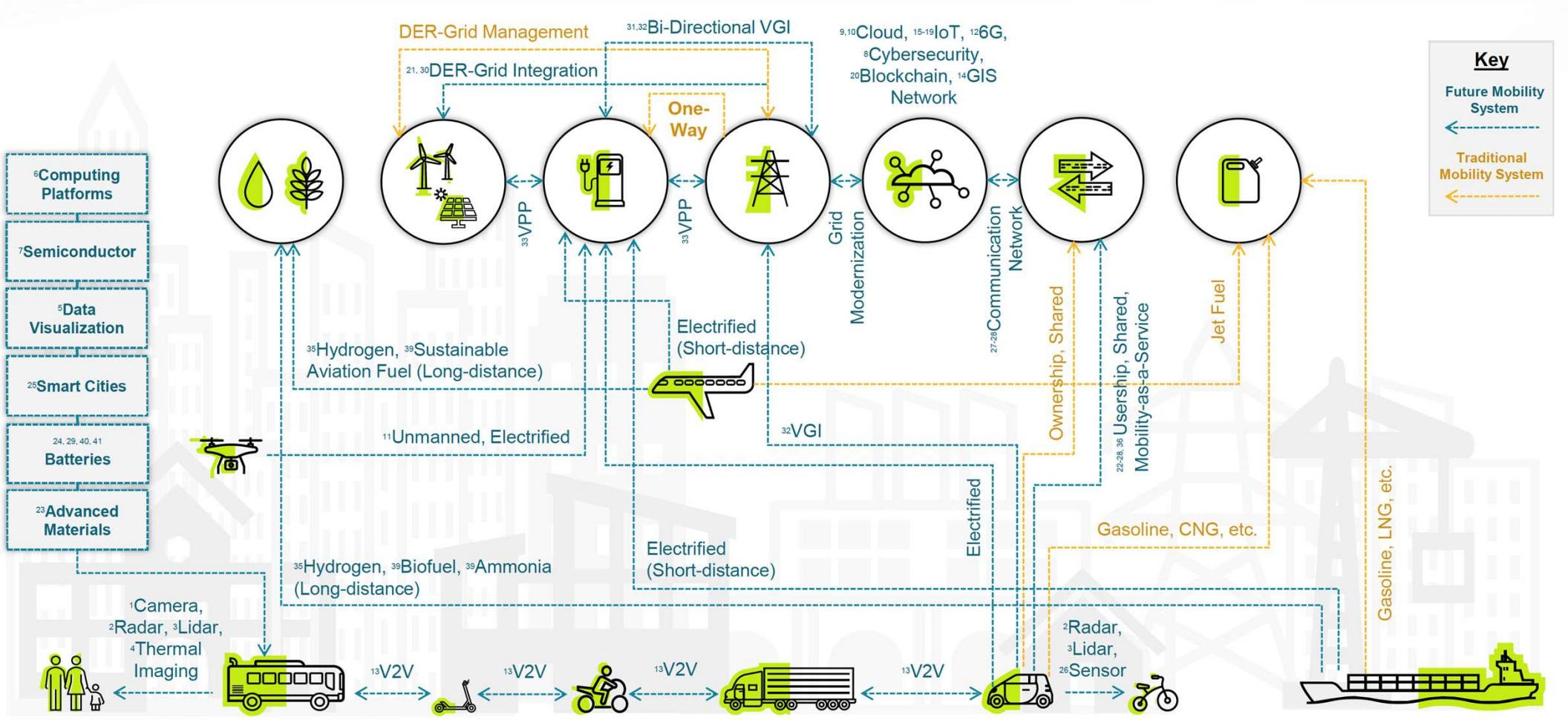
SOCIETAL MOBILITY

The future of mobility will affect everyone, whether they own cars, ride public transportation, rent e-scooters, or depend on products that were shipped to them from across the world. Our researchers are studying how **people and goods move** today, in order to strengthen the nation's transportation **policies, systems, and infrastructure** of tomorrow.

Learn about Economics & Infrastructure ····>

Learn about Moving People & Goods Research ····>

Research Landscape



Any Questions?

Contact information:

Kevin Heaslip
kheaslip@utk.edu
865-974-1813

Announcements

ISOAG August 6, 2025

VITA - CSRM Governance Welcomes two analysts!

We would like to extend a warm welcome to our new governance analysts: Kaffy Iyanda and Jelani Lynch

International Travel

As traveling season approaches us, lets make sure we all understand how to comply with COV guidelines regarding devices.

Before your trip, be sure to check out the knowledge base article on the VCCC site if you are travelling internationally.

If you're unsure about any compliance requirements, don't hesitate to ask!

WE WANT YOUR LOGS:

VITA is working with agencies to ingest their application logs in to the VITA Splunk instance. We ask that all agencies start identifying what logs you would like to have ingested. We are always happy to schedule a call to review your options.

Top 5 Vulnerabilities

For the month of August, the Top 5 Key Vulnerabilities are:

- **Apache Log4j SEoL < 1.x**
- **Apache Log4j 1.x Multiple Vulnerabilities**
- **Mozilla Foundation Unsupported Application Detection (Firefox)**
- **MS10-031: Vulnerability in Microsoft Visual Basic for Applications (978213)**
- **IBM WebSphere Application Server (6258333)**

NOTE Check CSRM Connections for more detailed information

Acunetix Survey

- **Survey Name:** Acunetix 360 Customer Satisfaction Survey
- **Survey Link:** https://forms.office.com/g/K8PbAKrcC5
- **Available From:** August 7, 2025 through August 22, 2025
- **Why should ISOs do it?** It'll help us spot any gaps and see how the product is performing, so we can make it even better.

Upcoming Events

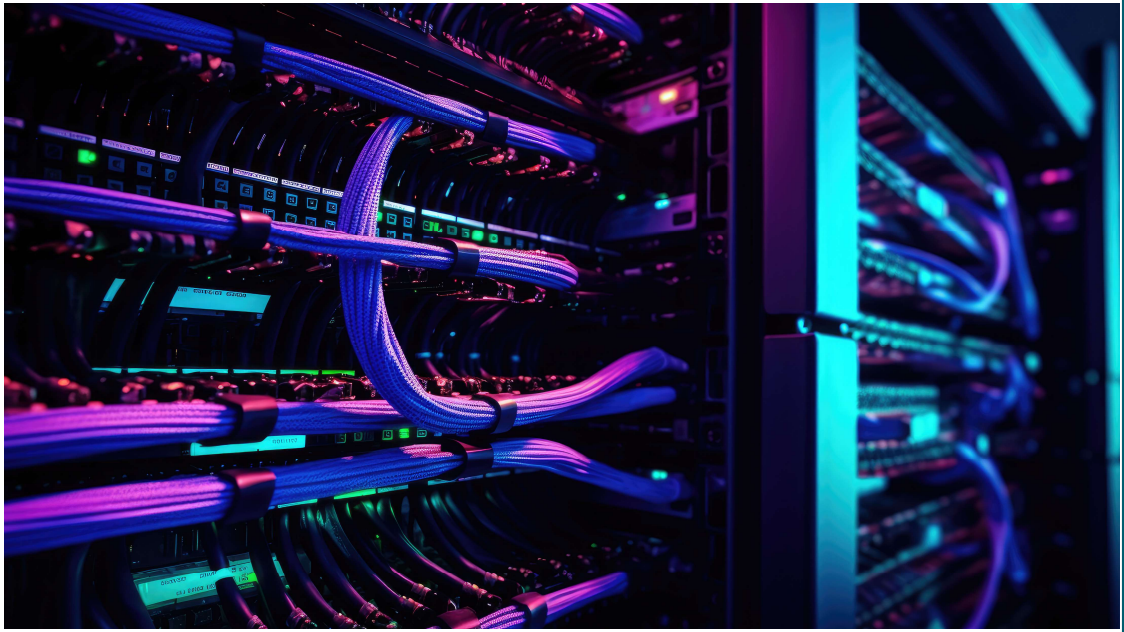
VIRGINIA
IT AGENCY
vita.virginia.gov

Governance Office Hours Announcement

Governance Office Hours launch recently – a dedicated space for Agency ISOs and teams to bring their questions, concerns, or ideas directly to the Governance Team.

What to Expect:

- **Open discussion place**
- **Governance Updates**
- **Q&A and support for your needs**



Next Session:
August 13th, 2025 | Microsoft Teams
[Click here to join the meeting]

Let's work together to strengthen governance across the Commonwealth!

Commonwealth of Virginia Information Security Conference 2025

ISC:25

Future-Proofing Cybersecurity: *Next-Gen Strategies*

August 14, 2025

Earn 5 CPE credits!

(Registrations after this date will require a handwritten badge)

Security Conference | Virginia IT Agency

Registration page

COVITS

[To register]

Service Tower SOC Report Review Sessions

The upcoming SOC review session is September 18, 2025, and will be held remotely.

Please register at the link below

To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/r356265cb4b5d84cfa98903fb0adb74f2

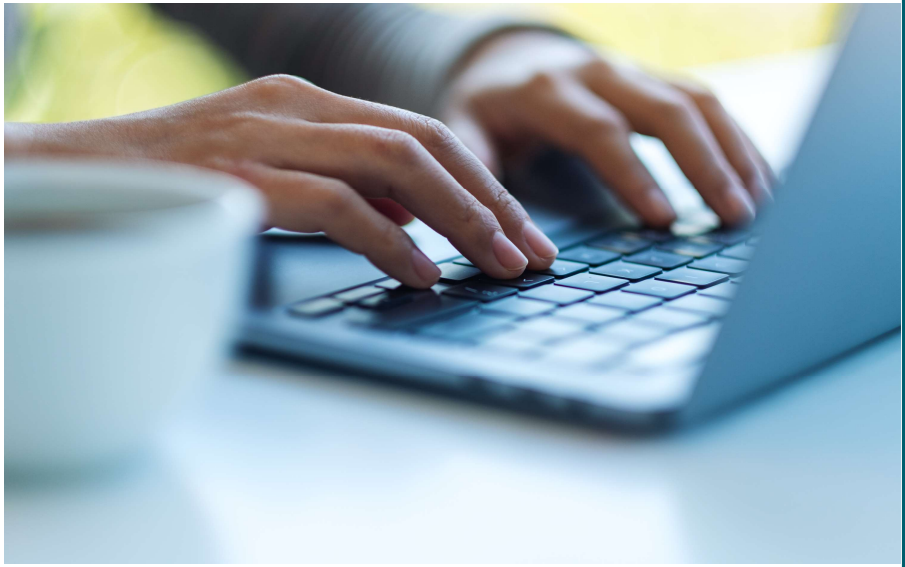
IS Orientation

The next IS Orientation is being held on September 24, 2025

- September 24, from 9am to 4pm, registration closes Sept 17th.
- It will be held in-person at the Boulders location:

  7325 Beaufont Springs Drive, Richmond, VA 23225

- Visit Commonwealth IS Orientation to register!



The October 1, 2025 ISOAG Meeting will be In-Person (and virtual)

Location: Reynolds Community College

Time: 1-4 pm

Please remember that in-person attendance is mandatory for primary, in-scope ISOs to maintain credentials. If one is unable to attend, you must let CSRM know and email who the designated person to come in that place is by September 17.

MEETING ADJOURNED

VIRGINIA
IT AGENCY