2024
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

5G Impacts to Vehicles and Highway Infrastructure:

A Comprehensive Narrative

(Image generated by AI platform Google Gemini, while utilizing an in-vehicle 5G WiFi network, based on user-provided descriptions…it seemed fitting for this paper)

Table of Contents

*We extend our deepest gratitude to the individuals and agencies who generously supported our research during our time in Orlando and joining us on our team calls. Special thanks go to the dedicated officials at **Orlando City Hall** and the neighboring **City of Altamonte Springs**, whose insights into local transportation and urban planning were invaluable. Their dedication and pride in advancing their city through innovative solutions and smart city initiatives were truly inspiring. We are particularly grateful to the **Florida Department of Transportation (FDOT)** for granting us access to the **SunTrax test facility**, where we gained hands-on experience with advanced automotive and transportation technologies. Our appreciation also goes to **Ariane Fikki,** Senior Director of Partnerships for the VR/AR Association, and the team at the **Institute for Simulation and Training (IST) at the University of Central Florida's School of Modeling Simulation & Training**, for their exceptional demonstrations of mixed reality technologies. The collective expertise and hospitality of these individuals and organizations greatly enriched our understanding and have significantly contributed to the success of our research. Their commitment to fostering smart city advancements and enhancing urban mobility showcases their forward-thinking approach and dedication to creating a better future. Thank you for your unwavering support and collaboration.*

Would also like to extend a heartfelt thanks to this incredible TEAM for their unwavering dedication and tireless efforts in developing this outstanding paper. Your commitment to excellence, from conducting thorough research to meticulously analyzing data, has been truly remarkable. Each team member's contribution, be it in writing, reviewing, or providing critical insights, has been invaluable. Your collaboration, creativity, and relentless pursuit of high standards have culminated in a comprehensive and insightful narrative on the impacts of how our topic comprehensively impacts 5G technology. Thank you for your time, resources, and exceptional teamwork. This paper is a testament to YOUR collective hard work and shared vision. On to PHASE 2!

The TEAM (in last name alphabetical order):

Mr. David Beckwith	United States Secret Service
Mr. William Black	CSX Technology
Mr. Virgil (David) Dafinoiu	AT&T Inc
Mr. Thanh (Tino) Dinh	Cherokee Federal Inc
Mr. Franbi Franco	Federal Highway Administration
Mr. Andrew Miller	MedAire
Mr. Rob Petrosino	Fifth and Cor
Mr. Matthew S.	Federal Bureau of Investigation
Mr. Malcolm Springer	Cybersecurity and Infrastructure Security Agency
Mr. Duminda Wijesekera	George Mason University
Dr. Charlesa Young	U.S. Government

Mr. Jason Carnes (Team Champion and biggest fan of this group!) Federal Highway Administration

Executive Summary

The fifth generation of mobile networks, commonly referred to as 5G, is a technological advancement that promises significantly faster data download and upload speeds, wider coverage, and more stable connections. The deployment of 5G technology is poised to transform the automotive industry and highway infrastructure. With its capabilities for faster data transmission, lower latency, and enhanced connectivity, 5G will facilitate advanced vehicle automation and smarter infrastructure systems, thereby giving rise to 'connected vehicles.' These advancements are expected to enhance traffic management, reduce accidents, and improve overall user experiences. However, the integration of 5G technology also introduces a new set of cybersecurity and supply chain security challenges that must be managed comprehensively. Finally, not necessarily intended to be left at the end – continued investment in educational opportunities within STEM disciplines and continuity planning to ensure a strong talent pool should be a consideration within all levels of this document's considerations.

Summary of Recommendations

For Government:

Develop and Enforce Uniform Regulatory Frameworks:

Establish national-level regulations to ensure uniformity across states, preventing jurisdictional conflicts and facilitating the seamless deployment of 5G-enabled transportation technologies.

Coordinate efforts between agencies such as the Department of Transportation (DOT), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Communications Commission (FCC) to address overlapping jurisdictions and streamline regulatory processes.

Facilitate Public-Private Collaboration:

Convene industry experts, academic institutions, and government agencies to share knowledge, best practices, and emerging threats.

Promote partnerships through funding, regulatory incentives, and policy frameworks that encourage innovation and enhance cybersecurity measures.

Invest in Advanced Security Measures:

Implement advanced encryption, authentication protocols, and intrusion detection systems to safeguard 5G networks and connected vehicle systems.

Leverage Software Bills of Materials (SBOMs) to enhance supply chain security and ensure transparency in the software components used in 5G systems.

Support Workforce Development:

Invest in STEM education and training programs to prepare the workforce for the demands of the evolving transportation and technology sectors.

Encourage continuous professional development and certification programs for security and technology professionals.

For Private Sector:

Integrate Security from the Outset:

Adopt a Secure Development Lifecycle (SDL) approach to embed cybersecurity measures in the design and development phases of products and systems.

Conduct comprehensive risk assessments and threat modeling specific to automotive and roadway systems.

Enhance Threat Intelligence and Detection Capabilities:

Implement real-time threat detection systems utilizing machine learning and artificial intelligence to monitor and respond to anomalies and potential cyber threats.

Incorporate threat intelligence feeds to stay updated on the latest attack vectors and vulnerabilities specific to 5G environments.

Promote Interoperability and Standardization:

Collaborate with industry peers and regulatory bodies to develop and adhere to common standards for data formats, communication protocols, and cybersecurity measures.

Participate in testing and certification programs to ensure products and systems meet established security and interoperability standards.

Foster Innovation and Investment:

Invest in research and development to explore new applications of 5G technology in transportation, including autonomous vehicles and smart infrastructure.

Engage in pilot projects and real-world testing to assess the effectiveness of new technologies and gather valuable insights for broader implementation.

Address Privacy and Data Security Concerns:

Establish clear guidelines for data collection, storage, and sharing to protect user privacy and comply with regulatory requirements.

Ensure transparency in data usage and provide consumers with control over their personal information.

Introduction and Scope of Research and Implications of Wireless Attacks on 5G Networks and Connected Vehicles

The project's research focused on wireless attacks as the main attack vector potentially impacting 5G networks, connected vehicles, and associated infrastructure. Connected cars primarily communicate wirelessly, but there are exceptions. An example is when an electric vehicle is connected to the power supply and communicates with the power grid or another back-end infrastructure. Potential vulnerabilities associated with physical connections between connected cars and energy infrastructure were not included in this project. The impacts of these wireless attacks could be significant, potentially

leading to critical sensor errors, navigation failures, and privacy breaches. In worst-case scenarios, national security could be at risk if threat actors target the driving functions of connected vehicles to carry out attacks against civilians or critical infrastructure. Additionally, these vulnerabilities can compromise the overall safety and reliability of smart transportation systems, affecting traffic management and public trust in emerging technologies.

Connected cars, in essence, are “phones with wheels” that combine the traditional risks of a moving vehicle with the potential security vulnerabilities associated with wireless mobile devices. The complexity of today’s vehicle operating systems could expose vehicles to previously unimaginable wireless attacks with privacy and safety implications. For example, a cyber-attack on a connected vehicle can result in critical sensor errors or navigation failures, resulting in vehicle collisions. In a worst-case scenario, national security threat actors could target the driving functions of connected vehicles to carry out vehicle-borne attacks against civilians or critical infrastructure.

The deployment of 5G technology enables real-time communication between vehicles (V2V) and between vehicles and infrastructure (V2I). This real-time data exchange is crucial for the development and deployment of autonomous vehicles and smart infrastructure. It supports more efficient traffic management systems, which can significantly reduce traffic congestion and accidents. For example, vehicles can communicate with each other to avoid collisions, and traffic signals can adjust in real-time based on current traffic conditions.

Summarization: Types of Vulnerabilities Potentially Impacting Connected Vehicles and Infrastructure

Despite the benefits of 5G integration with connected cars and infrastructure, the increased dependency on connectivity also heightens the risk of cyber-attacks. Malicious actors could exploit vulnerabilities in the communication networks to disrupt vehicle operations, infrastructure services, or steal private data. In addition, risks to supply chains and the source of individual components used to manufacture connect cars, smart roads, and other transportation infrastructure must be consider as a vulnerability.

Policy/Regulatory Categories:

1. **Evolving Mobility and Regulatory Push**: The rapid evolution of mobility, driven by innovations such as connected vehicles and urban mobility solutions, highlights the importance of regulations like the EU's "Fit for 55" program and the Biden administration's EV targets for 2030. These regulatory changes are essential for transforming the automotive industry into a domain of sophisticated connected entities.
2. **Need for Regulatory Uniformity**: The transition to connected and autonomous vehicles necessitate a common set of regulations, standards, and policies. Without a uniform national regulatory framework, achieving nationwide commercialization and leveraging 5G technologies will be challenging. Regulatory uniformity is crucial to avoid state-specific conflicts and ensure cohesive cybersecurity practices.
3. **Jurisdictional Complexity**: The regulatory landscape for automotive cybersecurity is complicated by overlapping jurisdictions of various governmental entities, such as the DOT, DHS, and FCC. Clear coordination and regulatory guidelines are essential to avoid gaps and overlaps in

cybersecurity measures, particularly with the integration of 5G technology. The US follows its own standards, such as FMVSS, rather than international regulations like those from UNECE.

Cybersecurity Risks: To mitigate cybersecurity risks, integrating security measures from the earliest stages of product development is crucial. This includes adopting an SDL, ensuring supply chain security, and developing advanced threat detection and incident response mechanisms. Collaboration between industry and government is vital for sharing threat intelligence and best practices.

Trade-offs: Balancing interoperability with cybersecurity, managing supply chain risks versus cost and availability, and weighing the pros and cons of connected transportation and autonomous vehicles are critical considerations. The development and deployment of connected and autonomous vehicles also stimulate STEM talent and investment, fostering innovation and economic growth.

Emerging Technologies: 5G-enabled, connected, and autonomous vehicle systems encompass a wide range of applications, including public transit, first responder vehicles, micro-mobility solutions, commercial trucking, and passenger vehicles. Each application presents unique challenges and opportunities, necessitating robust cybersecurity measures to ensure their safe and reliable operation.

The Future: The federal government can play a central role in facilitating the adoption of common technical interoperability and cybersecurity standards. By convening ecosystems and industry groups, sharing knowledge from innovation pilots, and establishing interagency working groups, the government can support the development of smart transportation infrastructure. Additionally, leveraging existing industry groups and testing facilities can help identify and mitigate vulnerabilities in complex systems.

Main Topics:

Policy and Regulatory Considerations

As the traditional concept of mobility is evolving rapidly, with innovative solutions designed for connected vehicles and urban roads, such as mobility-as-a-service and advanced traffic management systems, these innovations are being driven by changes in regulation, consumer behavior, and technology. For instance, the European Union's "Fit for 55" program and the Biden administration's EV targets for 2030 underscore the regulatory push for this transformation.

The automotive industry, once a realm dominated by mechanical prowess, is steering into uncharted territories by transforming vehicles into complex digital platforms. This shift is redefining the essence of vehicles from isolated mechanisms to sophisticated connected entities.

It is predicted in the near future, vehicles will be capable of communicating with each other in real-time, exchanging data, and making split-second decisions about speed, direction, and route. Considering the implications of autonomous driving, where the need for human intervention diminishes, and the vehicle becomes an intelligent entity capable of learning, adapting, and interacting with its environment.

The journey that 5G is initiating for the automotive industry is not just about speed; it's about connectivity, redefining safety, and enhancing the overall driving experience. It's about cars that can sync with your office calendar, schedule meetings on the go, or allow you to join a video conference from the comfort of your driver's seat.

Connected vehicles, therefore, have multiple implications for automakers to include: the need to focus on cybersecurity and data management; design new business models; boost investments in technology R&D; anticipate and address changing customer expectations; and collaborate with technology providers in order to stay abreast of the latest automotive technologies. Most importantly, there this is the urgent need for a common set of regulations, standards, and policies to govern the rapidly evolving, technology-driven connected vehicle industry.

Without a uniform, national-level regulatory framework, nationwide commercialization will be difficult to achieve. As automakers look to advanced technologies that can leverage 5G and improve their forthcoming vehicle models and services, the need for regulatory uniformity will be further emphasized.

Absent federal rules, US state legislators and regulators will be left to form state-specific regulations which could create conflicts between jurisdictions. Additionally, NHTSA has only recommended cybersecurity best practices which leads to a situation where OEMs can disregard the best practices altogether.

For instance, eCall, (an initiative by the European Union, **intended to bring rapid assistance to motorists involved in a collision anywhere within the** European Union) functionality is currently mandated in Europe but not in North America.

- *Jurisdictional Complexity*
    - The regulatory landscape for automotive cybersecurity is complicated by the overlapping jurisdictions of various governmental entities. While the USDOT has regulatory authority over vehicle safety, cybersecurity aspects often fall under different agencies, such as the DHS and the FCC. Coordinating these efforts and establishing clear regulatory guidelines are essential to avoid gaps and overlaps in cybersecurity measures, especially with the advent of 5G technology.
    - There are a uniform set of regulations under the UNECE World Forum for Harmonization of Vehicle Regulations. In North America, the US is not signatory to this nor does it recognize UN type approvals. Instead, it has its own mechanism – the FMVSS. Canada has the Canada Motor Vehicle Safety Standards that is broadly similar to FMVSS. However, the Comprehensive Economic and Trade Agreement between Canada and Europe could potentially make UN Regulations acceptable alternatives to the Canadian regulations.

Connectivity Regulation Snapshot

Region	Country	Data Privacy Regulations	Cybersecurity Regulations	SW Management Regulations	Functional Safety Regulations
North America	Canada	Protection of Personal Information and Electronic Documentation Act	Outlines for vehicle cybersecurity guidance but no implementation	No regulations so far	ISO/SAE and WP.29 Regulations
	United States	Certain states have adopted their own data protection laws (CCPA—California, Nevada Privacy Law—Nevada)	No regulations so far, NHTSA suggests cybersecurity best practices	No regulations so far, states intend to adopt their own over-the-air (OTA) regulations (Virginia, West Virginia)	ISO/SAE Regulations, NHTSA, FMVSS
European Union	All Member Countries	GDPR	UNECE WP.29 R155 Cybersecurity Management System (CSMS)	UNECE WP.29 R156 SW Update Management System (SUMS)	ISO/SAE and WP.29 Regulations, ASPICE
LATAM	Brazil	General Data Protection Law	National Cybersecurity Strategy (E-Ciber) offers a roadmap, but no implementation	No regulations so far	ISO/SAE Regulations, INMETRO certification and homologation
APAC	Japan	Act on Protection of Personal Information (granted GDPR adequacy)	UNECE W.29 R155 (CSMS)	UNECE W.29 R156 (SUMS)	ISO/SAE and WP.29 Regulations, ASPICE
	South Korea	Personal Information Protection Act (granted GDPR adequacy)	UNECE W.29 R155 (CSMS)	UNECE W.29 R156 (SUMS)	ISO/SAE and WP.29 Regulations, ASPICE
Asia	China	Personal Protection Information Law (PPIL)	Internet of Vehicles (IOV) Industry Standard for ICV Subpart 202-21	IOV Industry Standard for ICV Subpart 202-22	China Compulsory Certification homologation, ISO/SAE Regulations
	India	Personal Data Protection Bill	No regulations so far but intends to implement WP.29	No regulation so far but intends to implement WP.29	ISO/SAE Regulations

Active Regulation/Mandates *Pending/Partial Regulation* *No Regulation or Standard*

SAE: Society of Automobile Engineers; WP.29: UNECE World Forum for Harmonization of Vehicle Regulations; FMVSS: Federal Motor Vehicle Safety Standards; ASPICE: Automotive SW Process Improvement Capability Determination; INMETRO: National Institute of Metrology, Standardization, and Industrial Quality

Source: Frost & Sullivan

Public-Private Collaboration

Effective cybersecurity for 5G-enabled vehicles and infrastructure requires collaboration between public and private sectors. Policymakers should encourage partnerships that facilitate information sharing, joint research, and development of innovative security solutions. Public-private collaboration can help identify emerging threats, share best practices, and develop coordinated responses to cybersecurity incidents. Government agencies can provide support through funding, regulatory incentives, and policy frameworks that promote collaboration.

5G-enabled mobility and smart transportation spans multiple industry sectors. Some industries have formed alliances to articulate frameworks and areas for future innovation and collaboration. For example, the Alliance for Automotive Innovation and the Cellular Telecommunications Industry Association produced a recent 2024 report, "How 5G Is Driving the Auto Industry Forward[1]". These industry trade organizations predict that three 'mega trends' of how 5G can transform the world of mobility are "electrification, automation, and connectivity". They call on the FCC to grant additional 5G

[1] How-5G-is-Moving-the-Auto-Industry-Forward.pdf (ctia.org)

spectrum to realize the full efficiency and safety benefits that 5G-enabled smart transportation can offer[2].

Building a robust, reliable, and cybersecure broadband telecommunications infrastructure requires public private collaboration. At the same time, federal agencies must also enforce the appropriate regulatory regime on affected industries, including telecommunications, automotive and other vehicle manufacturers, electronic communications hardware and software providers, and road engineering and construction firms. The American public requires public and private sector actors to work in good faith to anticipate and work through the trade-offs of public safety, innovation, and cost.

Federal funding has expanded in recent years to develop a 5G network nationwide, such as new broadband programs funded by the Bipartisan Infrastructure Law[3] and administered by the NTIA[4] and investments to enhance 5G capabilities on FirstNet, also an NTIA agency[5]. A 2019 McKinsey report lays out similar trends[6]. CISA has published many security resources and facilitates information sharing on cybersecurity threats, including 5G-specific risks[7].

For the specific topic of managing the safe, reliable, inter-operable, and cyber-secure roll out of 5G-enabled connected transportation technologies, the US federal government should form an inter-agency body which preforms outreach to industry and academic experts. This body would ideally operate in a holistic and coordinated manner with the technical expertise and authority to represent the interests of the American public. These parties may disagree as was the case between FCC and USDOT on spectrum use for vehicle safety[8]. This is especially true, since 5G-enabled connected transportation spans the regulatory jurisdictions, federal grant and incentive programs, and R&D funding across numerous federal, state, and local agencies. An inter-agency body could consist of, but not limited to, the following agencies:

- U.S. Department of Transportation: FHWA, FMCSA, NHTSA, FAA, FTA
- Department of Homeland Security: CISA
- Department of Commerce: NTIA, NIST
- Federal Communications Commission (FCC)

This inter-agency body could help the federal government conduct the following activities.

- **Federal Government as Central Convener**
    - **Facilitate Adoption of Standards:** The federal government can play a central role in facilitating the adoption of common technical interoperability and cybersecurity standards across industry and state/local communities. This can be achieved through grant requirements and providing resources for local contracting and cybersecurity officials.

---

[2] Four ways 5G is driving change in the automotive industry (rcrwireless.com)
[3] Biden-Harris Administration Allocates More Than $800 Million to Increase Digital Inclusion Efforts | National Telecommunications and Information Administration (ntia.gov)
[4] Broadband Grant Programs | National Telecommunications and Information Administration (ntia.gov)
[5] 5G on FirstNet: More data, greater speeds in near real time | First Responder Network Authority
[6] 5G cars and the mobility technology ecosystem | McKinsey
[7] 5G Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA
[8] Smart Cars and Trucks: Spectrum Use for Vehicle Safety (congress.gov)

    - **Convene Ecosystems and Industry Groups:** By convening industry subject matter experts, the federal government can facilitate the sharing of knowledge and lessons learned from innovation pilots nationwide. This will help identify common interests and concerns, informing future regulation, legislation, and programs.
    - **Interagency Working Group:** Establishing an interagency working group or task force can continue these efforts, spanning the USDOT, CISA, NTIA, FCC, FirstNet, FAA, and local governments. Alternatively, leveraging existing networks like CISA and DHS Fusion Centers can be effective for knowledge sharing.
    - **Resources and Guidelines:** Rather than central planning, the federal government can provide resources and guidelines that local governments and industry will find useful.

- **Leverage Existing Industry Groups and Associations**
    - As part of a 'Smart Cities/Connected Transportation' alliance, existing industry groups and associations can encourage the adoption of common interoperability and cybersecurity standards. Engaging citizens and lawmakers in this process is also essential.

- **Facilitate Systems Testing**
    - Bringing together red teams, ethical hackers, systems integrators, and local government operations and planning staff can facilitate testing of cyber-physical interfaces. Moving beyond table-top exercises to real-world test ranges or digital twin simulations can provide valuable insights.
        - **Ethical Testing:** Conducting red team, white hat, and ethical testing of cyber and physical security vulnerabilities is crucial. Facilities like SunTrax can convene vendors and local governments to test multiple systems working together.
        - **Vetting Participants:** Ensuring thorough vetting of companies, individuals, and other participants involved in testing is essential for maintaining security.

- **Privacy Protection**
    - With the increased data exchange facilitated by 5G networks, protecting the privacy of vehicle users is a significant concern. Regulatory frameworks must ensure that personal data collected through V2X communications is adequately protected. This includes establishing guidelines for data collection, storage, and sharing, as well as enforcing strict privacy protection measures. Transparency in how data is used and the ability for consumers to control their data are essential components of privacy protection in the connected transportation ecosystem.

Trade-offs

The impacts of 5G-enabled connected and autonomous transportation system will require careful analysis and foresight of potential trade-offs for regulators, manufacturers, operators, and passengers. The following are some of the major trade-offs.

Interoperability vs. Cybersecurity

Interoperability is essential for the seamless communication between various vehicle systems and infrastructure components. However, achieving high levels of interoperability often requires opening up systems to external connections, which can increase cybersecurity vulnerabilities. Balancing the need for interoperability with robust cybersecurity measures is a critical challenge. Ensuring that systems can

communicate effectively without compromising security involves implementing standardized protocols and rigorous security testing.

Furthermore, the competitive nature of the telecom and automotive industries places protecting intellectual property before developing common industry standards and sharing knowledge of vulnerabilities. It may take a neutral part, whether a US federal agency like NIST or a non-profit industry consortium to incentivize the adoption of common interoperability and cybersecurity standards. Furthermore, common standards and open architectures must also be developed with resilience in mind. The Crowdstrike incident of July 19, 2024[9] highlights the fragility of highly interconnected systems and the risks posed universally uniform technology standards, poor software quality controls and industry concentration[10], much less malicious cybersecurity breaches.

Supply Chain Risk Management (SCRM) vs. Cost and Availability

Managing risks within the supply chain, especially when critical components are sourced from regions with different security standards, presents a significant challenge. Many components, including controllers and other critical parts, are manufactured in China. Local governments may not have the budget or bandwidth to thoroughly vet these vendors, and there is often immediate pressure to field functional, reliable, and affordable equipment. This trade-off between ensuring secure supply chains and managing costs and availability requires a balanced approach. Investment in vetting suppliers and developing local capabilities can help mitigate risks while maintaining cost-effectiveness.

Federal agencies including CISA[11], US Customs and Border Protection[12], and Commerce[13] are working through guidance related to ICT supply chain risk management to increase transparency for sensitive electronic components needed for 5G-connected transportation systems. Decreasing cost and increasing availability of electronic components and necessary products for connected transportation will require trade policies to diversify sources from China and industrial policies to build up domestic manufacturing capabilities—unfortunately, such efforts are unlikely to keep pace with near term passenger demand.

Pros and Cons of Connected Transportation/Autonomous Vehicles

Innovation vs. Consumer Demand: The demand for innovative transportation solutions is driven by consumer needs for multi-modality in people and goods delivery. Balancing individual consumer choice with the public good requires careful management and regulation. The inevitability of innovation in transportation technology necessitates proactive planning and policy development to ensure that the benefits are maximized while mitigating potential downsides.

This transportation planning effort is highly localized and best conducted by local-level agencies and organizations. As this AEP group discussed with officials from Orlando City Hall and observed first-hand

---

[9] Flights, banks and media hit as internet users report global outages | AP News
[10] Tech Disruptions Sparked by Software Update Highlight the Fragility of Globally Connected Technology (usnews.com)
[11] ICT Supply Chain Risk Management Task Force | CISA
[12] CBP Launches Global Business Identifier Pilot to Increase Supply Chain Visibility | U.S. Customs and Border Protection
[13] ICT Supply Chain | U.S. Department of Commerce

in the neighboring city of Altamonte Springs, local transportation and urban planning officials are iteratively deploying and testing various modes of autonomous and electric vehicles, 'micro-mobility' solutions such as electric scooters and bicycles, and even drones, all operating in the same urban environment. The AEP group visited the SunTrax test facility[14], operated by FDOT and offered for use by companies and universities to test advanced automotive and transportation technologies. These innovation pilots and tests are necessary for uncovering risks and for incorporating public feedback.

Importance of Interoperability for 5G-Enabled Transportation

Vehicle and Infrastructure Interoperability:

Achieving interoperability between various vehicle systems and highway infrastructure components is critical for the success of 5G-enabled transportation. Policymakers and regulators need to develop and enforce standards that ensure seamless communication and compatibility between different manufacturers' systems. This includes setting guidelines for data formats, communication protocols, and cybersecurity measures that all stakeholders must adhere to. Standardization will help mitigate cybersecurity risks and ensure the reliable operation of connected transportation systems.

Interoperability is essential for the successful implementation of 5G-enabled transportation systems because:

- **Enables seamless communication:** Different vehicle systems and infrastructure components must communicate effectively and efficiently to exchange information. Interoperability ensures this seamless exchange.
- **Facilitates data sharing:** Various stakeholders, including vehicle manufacturers, infrastructure providers, and government agencies, must share data for applications like traffic management, autonomous driving, and emergency services. Interoperability allows for smooth data transfer and utilization.
- **Promotes innovation:** A standardized and interoperable environment fosters innovation by allowing different companies and organizations to develop and integrate new technologies and services without compatibility issues.
- **Improves system efficiency:** Interoperability reduces complexities and inefficiencies arising from incompatible systems, leading to optimized resource utilization and better overall system performance.
- **Enhances safety & security:** Interoperability is crucial for ensuring the reliable and safe operation of connected vehicles and infrastructure, as it enables timely communication and coordinated actions in case of emergencies.

Development of Standards

- Creating a clear and comprehensive framework for the development of interoperability standards. Encouraging collaboration between industry, academia, and government agencies to develop standards that meet the needs of all stakeholders. Identifying critical areas for

[14] Innovative SunTrax Center Celebrates Grand Opening - SunTrax (suntraxfl.com)

standardization, such as data formats, communication protocols, and cybersecurity. Investing in research to advance the development of new standards and technologies.

Enforcement of Standards

- Implementing regulations that require compliance with established interoperability standards, developing mechanisms to certify products and systems that meet the required standards, enforcing compliance through penalties for non-adherence to standards, continuously monitoring the effectiveness of standards, and making necessary adjustments.

Guidelines for Data Formats

- Enforcing standardized data formats to ensure compatibility between different systems and applications, promoting data sharing initiatives while preserving privacy and security, establishing guidelines for data accuracy, completeness, and reliability, and ensuring that data is accessible to authorized parties for research, development and public benefit.

Guidelines for Communication Protocols

- Mandating the use of open and interoperable communication protocols, requiring the implementation of strong security protocols to protect data transmission, efficiently allocating spectrum for transportation-related communication services, and establishing standards for network reliability and performance.

Improved Interoperability

- Standardization ensures that different components and systems can communicate effectively and efficiently. Standardized data formats also facilitate the smooth exchange of information between vehicles, infrastructure, and other entities.

Increased System Reliability

- Standardized components and systems lead to more predictable system behavior, reducing the likelihood of failures. Standardization also helps minimize human error by providing clear guidelines and procedures. Standardized systems are also easier to diagnose and repair, leading to quicker recovery from issues.

Enhanced Safety

- Standardized components and systems are more likely to perform consistently, reducing the risk of accidents. Standardized communication protocols also enable faster and more effective emergency response.

Cost Efficiency

- Standardization can lead to economies of scale in production and maintenance. Standardized components and systems can reduce development costs by eliminating the need for redundant efforts.

Facilitated Innovation

- Standardization provides a common platform for innovation, allowing different companies to build upon existing standards. Standardized components and systems can also accelerate the development and deployment of new technologies.

Stimulating STEM Talent and Investment

The development and deployment of connected and autonomous vehicles create a demand for STEM talent and can stimulate investment and entrepreneurship. This growth can benefit the public good by fostering innovation and economic development. However, ensuring that the workforce is adequately prepared and that investments are directed towards sustainable and beneficial technologies is essential.

In particular, during our visit to Orlando, an FDOT engineer **highlighted the shortfall in civil engineers as a crucial bottleneck in sustaining and deploying innovation to current transportation networks.** Fortunately, other technologies have the potential to introduce transformative technologies that could offset the shortages of engineering talent deployed for public benefit. Thanks to Ariane Fikki, Senior Director of Partnerships for the VR/AR Association, we learned that the Orlando area is home to mixed reality and gaming companies such as Unity and MagicLeap. Ms. Fikki introduced us to the Institute for Simulation and Training (IST) at the University of Central Florida's School of Modeling, Simulation, & Training director. Visiting the many AR/VR, modeling & simulation, and digital twins technologies on display, we learned how these mixed reality technologies could help accelerate the development of 5G connected transportation and urban mobility solutions.

Risk

Product & Software Development

- The fifth generation (5G) of wireless technology introduces new connections, capabilities, and services, enabling billions of devices and applications. However, these advancements also bring significant risks that threaten national security, critical infrastructure, and the US economy. One key risk is the use of 5G components manufactured by untrusted companies, which could expose entities to malicious software, counterfeit components, and flaws due to poor manufacturing processes. Since 5G networks allow for numerous connected devices, traditionally insecure IoT devices may become vulnerable when integrated into this network. To mitigate these cybersecurity risks, it is crucial to integrate security measures from the earliest stages of product development. Adopting an SDL approach can help ensure that cybersecurity is embedded in the design and development processes. However, transitioning to an SDL model requires significant organizational changes and commitment from leadership. This involves training personnel, updating development practices, and continuously assessing and improving security measures.
- For organizations involved in deploying 5G technologies in vehicles and highway infrastructure, the stakes are particularly high. Manufacturers and entities deploying 5G technologies must prioritize integrating SDL practices to safeguard against the unique threats associated with this critical infrastructure. As a starting point, professionals supporting 5G rollouts should conduct comprehensive risk assessments and threat modeling specific to automotive and roadway systems. As 5G technologies become integrated, it's imperative that secure coding practices are followed and security tests are performed, to include penetration tests tailored to vehicular and infrastructure systems. Post-deployment, it's essential to implement continuous monitoring to quickly identify and address new vulnerabilities that could compromise vehicle safety or traffic management systems. Effective collaboration between teams and stakeholders is also vital to

maintaining high security standards and ensuring that systems remain resilient against evolving threats. By embedding SDL principles into every aspect of development and operational processes, security professionals can protect against potential security breaches and enhance the safety and reliability of 5G-enabled transportation networks.

- To further bolster security and manage risks, organizations can leverage SBOMs as a crucial tool. SBOMs provide a detailed inventory of all components, including open-source and third-party software, integrated into 5G systems. By utilizing SBOMs, security professionals gain enhanced visibility into the software supply chain, enabling them the track and assess the security of each component. This transparency helps to quickly identify and respond to vulnerabilities or compliance issues in the components used in vehicles and highway infrastructure. Additionally, SBOMs support better risk management by facilitating timely updates and patches for any identified security flaws. Implementing SBOMs as part of a SDL strategy can help ensure that all software components are secure and compliant, thereby strengthening the overall integrity and safety of 5G-enabled systems across infrastructure projects.
- It is essential to equip developers with the knowledge and skills necessary to implement secure coding practices. Training should cover principles such as input validation, proper error handling, secure data storage, and protection against common vulnerabilities like SQL injection and cross-site scripting. Regular workshops, coding exercises, and certification programs can help ensure that development teams remain proficient in the latest security techniques and practices, reducing the risk of introducing vulnerabilities into 5G-enabled systems.
- Compliance with industry standards and regulations is critical for ensuring the security and integrity of 5G technologies, particularly in automotive applications. For instance, the ISO/SAE 21434 standard provides guidelines for cybersecurity in the automotive industry, focusing on risk management throughout the lifecycle of vehicle systems. Additionally, NIST offers guidelines through its NIST Special Publication 800-53, which addresses security controls for federal information systems, including those related to connected vehicles. Ensuring compliance with these and other relevant standards helps mitigate risks and aligns with best practices for securing 5G technology in transportation infrastructure.

Cybersecurity

The automotive industry is undergoing a rapid transformation with the integration of advanced technologies like connected vehicles, autonomous driving, and over-the-air updates. This evolution has significantly increased the attack surface, making cybersecurity a paramount concern. To mitigate risks, a robust framework of cybersecurity standards is essential.

- **Cybersecurity Standards for Automotive Industry**
    - The automotive industry must adhere to stringent cybersecurity standards to protect against the increased vulnerabilities introduced by 5G connectivity. Regulatory bodies should work with industry stakeholders to develop comprehensive cybersecurity guidelines that cover the entire lifecycle of connected vehicles, from design and manufacturing to maintenance and decommissioning. These standards should include requirements for secure software development, regular security updates, and incident response protocols.

The Need for Strong Cybersecurity Standards

- **Protection of Sensitive Data:** Vehicles collect and store vast amounts of personal and vehicle data, making them attractive targets for cyberattacks.
- **Safety and Security of Drivers:** A compromised vehicle can seriously threaten the safety of occupants and other road users.
- **Economic Impact:** Cyberattacks on the automotive industry can lead to significant financial losses due to data breaches, product recalls, and reputational damage.
- **Consumer Confidence:** Strong cybersecurity measures are essential to build and maintain consumer trust in connected vehicles.

Key Cybersecurity Standards

Several standards and guidelines have been developed to address the cybersecurity challenges faced by the automotive industry:

- **SAE J3061:** This standard provides a cybersecurity framework for developing production vehicles. It covers requirements for threat analysis, risk assessment, and security controls.
- **ISO/SAE 21434:** This international standard focuses on cybersecurity engineering for road vehicles. It establishes a lifecycle approach to cybersecurity management, including requirements for the development, production, operation, and maintenance phases.
- **UNECE WP.29:** The United Nations Economic Commission for Europe (UNECE) Working Party on Vehicle Regulations has developed cybersecurity regulations for vehicle type approval.
- **NIST Cybersecurity Framework:** While not automotive-specific, the National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a comprehensive approach to managing cybersecurity risk.

Core Elements of Cybersecurity

To achieve a high level of cybersecurity, below are some measures the automotive industry should focus on:

- **Risk Assessments:** To prioritize mitigation efforts and evaluate the likelihood and impact of potential threats.
- **Threat Modeling:** Identifying potential threats and vulnerabilities to inform security measures.
- **Security by Design:** Incorporating security into the vehicle development process from the outset.
- **Secure Software Development:** Implementing secure coding practices and testing to prevent vulnerabilities.
- **Over-the-Air Updates:** Ensuring secure and reliable delivery of software updates to address vulnerabilities.
- **Incident Response:** Developing and testing incident response plans to minimize the impact of cyberattacks.

- **Continuous Monitoring:** Implementing ongoing monitoring and detection capabilities to identify and respond to threats.

5G Network Security

- As 5G networks become integral to vehicle-to-everything (V2X) communications, ensuring their security is paramount. Organizations involved in deploying and managing 5G technologies for vehicles and highway infrastructure must implement a suite of advanced security tools and controls tailored to the specific challenges posed by 5G connectivity.
- Advanced encryption is fundamental for securing data transmitted between vehicles and infrastructure within 5G networks. With 5G's capabilities such as increased data rates, and ultra-reliable low-latency communication the volume and sensitivity of data exchanged are considerably higher. To protect this data, implementing end-to-end encryption is essential. This involves using Advanced Encryption Standard (AES) with 256-bit keys to encrypt data at rest and Transport Layer Security (TLS) 1.3 for securing data in transit. Furthermore, encryption protocols should be updated to align with the latest standards, including recommendations from NIST for quantum-resistant algorithms like Post-Quantum Cryptography (PQC). This future-proofs the network against potential quantum computing threats. Encryption needs to encompass all communication forms within the 5G ecosystem, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-network (V2N) interactions, ensuring that all data exchanges are adequately secured.
- **Authentication protocols** are critical for validating the legitimacy of devices and users within the 5G network. Given the vast scale and complexity of 5G, which supports a massive number of connected devices and diverse applications, robust MFA mechanisms are imperative. This includes the use of PKI to issue and manage digital certificates for device and user authentication. Mutual authentication, where both the device and network validate each other, is crucial to prevent unauthorized access and spoofing attacks. In the context of 5G, the authentication process must address the needs of Software-Defined Networking (SDN), which require secure verification of virtualized network components and applications.
- **Intrusion Detection and Prevention Systems** (IDPS) are vital for safeguarding 5G networks from sophisticated cyber threats. These systems must be optimized for the high throughput and low latency of 5G environments. Advanced IDPS solutions leverage machine learning and artificial intelligence to perform real-time traffic analysis, detecting anomalies and patterns indicative of malicious activities. For example, deploying behavior-based anomaly detection can identify unusual traffic patterns in V2X communications that might suggest an active attack or system compromise. Network-based Intrusion Detection Systems (NIDS) monitor the flow of data across network boundaries, while Host-based Intrusion Detection Systems (HIDS) focus on securing individual devices. Integrating threat intelligence feeds into these systems enhances their capability by providing up-to-date information on emerging threats specific to 5G, such as new attack vectors and malware signatures.
- **Network slicing and segmentation** are advanced techniques that enhance security by isolating different types of traffic within the 5G infrastructure. Network slicing enables the creation of multiple virtual networks on a single physical 5G infrastructure, each customized for specific applications like V2X communications, emergency services, or IoT devices. This isolation ensures

that a security breach in one slice does not impact others, containing potential damage and reducing the overall attack surface. Implementing segmentation through VLANs (Virtual Local Area Networks) and VPNs (Virtual Private Networks) within each slice further strengthens security. For critical infrastructure, applying network function separation ensures that control plane functions and user plane functions are segregated, enhancing the network's resilience against attacks and operational failures.

Threat Intelligence and Detection

- Real-time threat detection and effective incident response mechanisms are critical for managing cybersecurity risks, especially in the context of 5G technologies for vehicles and highway infrastructure. The integration of 5G into automotive systems and transportation networks significantly increases the attack surface, making it imperative to have sophisticated systems in place to detect and respond to threats promptly.
- Investing in advanced threat detection systems is crucial for identifying and mitigating these threats before they escalate. For organizations involved in deploying 5G technologies in vehicles and highway infrastructure, this means implementing specialized security tools that are capable of handling the unique risks associated with 5G networks. These tools should include real-time monitoring systems that leverage machine learning and artificial intelligence to analyze traffic patterns and detect anomalies indicative of potential cyber threats.
- Additionally, integrating threat intelligence feeds into these security tools is essential for maintaining an up-to-date defense against emerging vulnerabilities. Threat intelligence provides valuable insights into the latest attack vectors, malware signatures, and hacking techniques that are specific to 5G environments. By incorporating this intelligence into your security infrastructure, you can enhance the capability of your threat detection systems to recognize and respond to novel threats more effectively.
- For example, incorporating threat intelligence can help identify patterns of attack that target 5G network components or exploit vulnerabilities in connected vehicles. This integration allows for the automation of threat detection processes, enabling quicker identification of suspicious activities and potential breaches. It also supports predictive analytics, which can foresee and mitigate potential threats before they manifest into significant issues.
- To effectively safeguard 5G-enabled vehicles and highway infrastructure, organizations must prioritize real-time threat detection and the integration of threat intelligence. By investing in advanced security tools and incorporating comprehensive threat intelligence, you can significantly enhance your ability to identify and address 5G security threats, thereby protecting vital transportation systems from evolving cyber risks.

Supply Chain Security

- The automotive supply chain is highly complex, involving numerous suppliers and third-party vendors, each representing a potential point of vulnerability. Ensuring the security of components and software from all suppliers is essential, necessitating the development and enforcement of standardized cybersecurity protocols and guidelines for end-to-end security. Implementing a software bill of materials can help track and manage the various software

components used in vehicles, making it easier to identify and address vulnerabilities. Supply Chain Security focuses on risk management of external suppliers, vendors, logistics, and transportation (Lewis & Wright, 2021)[15]. The rise of cybersecurity incidents underscores the importance of these measures. For instance, in January 2024, Hyundai Motor Europe experienced a security breach detected within their network by the "Catus Ransomware Group," which also attacked CIE Automotive, a prominent Spain-based automotive parts supplier (Yang, 2024)[16].

The possibilities of third-party vendor compromises, such as outdated/unpatched systems and embedded malware, have continued to rise because of the lack of standards and guidelines currently available. With the rise of autonomous vehicles being developed, the supply chain security risk will be even more prevalent as time goes on. The demand of autonomous vehicles are forcing the automotive industry to utilize multiple third-party vendors that are not being properly vetted for security concerns. This is concerning because vehicles are becoming more connected then ever before, and cyberattacks on vehicles can have a ripple effect impacting not only individual vehicles but also others who could be on the road.

- Additionally, implementing a software bill of materials can help track and manage the various software components used in vehicles, making it easier to identify and address vulnerabilities. Numerous gaps within the supply chain will require comprehensive evaluations to implement this bill. This bill will allow the automotive industry to better guard against vehicle vulnerabilities, while ensuring the safety of their customers' private information.

The Future

Learn Lessons from Global Innovators

Studying the approaches of global innovators like Singapore[17], Israel[18], South Korea[19], and Estonia[20] and the EU's 5G-PPP can provide valuable insights at the national-, city-, and company-level. Conversely, understanding the pitfalls of digital authoritarian systems like China can help identify what not to do, domestically and internationally.

Align US Industrial Policy

Aligning US industrial policy to facilitate the emergence of a domestic economy of smart cities manufacturers and service providers is crucial. Examples like the CHIPS Act and Science Act of 2022[21]

---

[15] Lewis, S. and Wright, G. (2021). Supply Chain Security. Retrieved from https://www.techtarget.com/searcherp/definition/supply-chain-security

[16] Yang, O. (2024). Emerging Threats to the Automotive Supply Chain From Ransomware Groups. Retrieved from https://vicone.com/blog/emerging-threats-to-the-automotive-supply-chain-from-ransomware-groups

[17] 5G Innovation | IMDA

[18] Second funding round winners for the 5G "Pilots Program" - English Innovation Site (innovationisrael.org.il)

[19] The year of future transportation: An interview with Seoul Mayor Park Wonsoon | McKinsey

[20] Estonian companies are evolving smart city solutions - e-Estonia

[21] R47523 (congress.gov)

can be accentuated to support smart transportation infrastructure and connect underserved communities. Ensuring economic and climate change resilience is also essential.

Re-imagine 'Smart Cities'

While the concept of 'smart cities' has faced criticism due to ethical concerns, cybersecurity, privacy, and corporate dominance[22], the mobility and transportation aspects of 'smart cities' continue to be deployed and to evolve[23]. Innovation is already happening organically through e-mobility, micro-mobility, EVs, semi-autonomous AVs, sUAS, and robotics. Local governments must manage these developments to protect public safety, privacy, commerce, and user choice.

The power dynamics are shifting from companies that invented the 'smart cities' concept to local residents and their local government representatives. As the AEP group learned from Orlando area city officials, engaging local citizens in the decision-making process is essential, but avoiding partisan divisions that paralyze planning is crucial.

Potential Multimodal Considerations with Impacts to Highway Modernization

Aerial Systems

The integration of 5G technology extends beyond ground vehicles to include various aerial systems.

- **Small Unmanned Aerial Systems (sUAS):** sUAS, commonly known as drones, benefit from 5G connectivity for improved control and data transmission. However, securing these connections against potential threats is critical.
- **Electric Vertical Takeoff and Landing (eVTOL) Vehicles:**
    - **Passenger:** eVTOL vehicles for passenger transport can alleviate urban congestion and provide new mobility options. Regulatory frameworks must address both cybersecurity and safety concerns.
    - **Cargo Delivery:** eVTOL cargo delivery systems can enhance logistics and supply chain efficiency. Ensuring the security of these systems is vital to prevent disruptions in goods delivery.
- **Regulatory Considerations:** Agencies like the FAA and USDOT must collaborate to develop regulations that address the unique challenges of aerial vs. ground transport, including cybersecurity standards and operational guidelines.

5G Technology in Aerial Systems

- The integration of 5G technology in aerial systems marks a significant advancement in aviation and UAV operations, providing enhanced connectivity and communication bandwidth. This development enables seamless data transmission between UAVs, ground stations, and other systems, facilitating real-time video streaming and data analytics. According to Supriya (2024)[24], 5G's ultra-low latency

[22] We Were Promised Smart Cities. What Happened? | Built In

[23] Tech transition 'is going to happen' despite 'smart city' scepticism (ft.com)

[24] Supriya, K. (2024, June 28). 5G Automation: Enhancing autonomous aerial vehicles and unmanned aerial systems for aerial imaging in 2024. Apeksha Telecom. https://www.telecomgurukul.com/post/5g-automation-enhancing-autonomous-aerial-vehicles-and-unmanned-aerial-systems-for-aerial-imaging-i

allows for instant transmission of high-resolution images and videos, crucial for applications such as aerial imaging, search and rescue operations, critical infrastructure inspections, and security surveillance. Live video feeds from autonomous aerial vehicles (AAVs) offer immediate information, supporting timely decision-making and environmental monitoring. Small Unmanned Aerial Systems (sUAS) benefit significantly from 5G integration, particularly through improved control. The high-speed and low-latency characteristics of 5G networks enable precise and responsive drone control in complex environments like urban areas. Becker (2022)[25] notes that most current commercial drone operations are restricted to the operator's line of sight (LOS), limiting their range. However, 5G technology facilitates beyond visual line of sight (BVLOS) operations, allowing sUAS to operate over greater distances with reliable connectivity, essential for expanding drone operations to tasks such as infrastructure inspections, delivery services, and environmental monitoring without LOS limitations.

Passenger Transport

- Urban Air Mobility (UAM) aims to revolutionize short-distance travel in congested urban areas using Electric Vertical Takeoff and Landing (eVTOL) vehicles, which operate below traditional flight altitudes to reduce ground congestion. UAM relies heavily on 5G connectivity for critical functions such as air traffic management, precise navigation, and real-time vehicle-to-vehicle communication, enabling eVTOLs to navigate complex cityscapes, avoid collisions, and maintain smooth traffic flow, significantly reducing travel times. However, the introduction of eVTOLs presents cybersecurity challenges, as aviation communication systems like ACARS can expose sensitive data to threats such as RF jamming, spoofing, and injection attacks. Effective countermeasures, reliable emergency communication systems, and seamless integration with existing air traffic control are essential to ensure the secure and efficient operation of UAM, ultimately transforming urban transportation while maintaining high safety standards.

Cargo Transport

- Electric Vertical Takeoff and Landing (eVTOL) cargo delivery systems are poised to revolutionize logistics and supply chain efficiency by providing faster, more direct delivery routes, especially in densely populated urban areas. Texeira (2024)[26] highlights that the vertical takeoff and landing capabilities of eVTOLs allow them to access challenging locations and deliver goods directly to customers, reducing delivery times and enhancing efficiency. This innovative approach streamlines logistics operations and sets new standards in urban air mobility, showcasing the transformative potential of eVTOL technology in improving the consumer delivery experience. However, the security of eVTOL cargo delivery systems is critical to maintaining supply chain integrity. Vulnerabilities could lead to disruptions like theft, tampering, or redirection of valuable cargo. Robust security measures, including securing data exchanges, safeguarding cargo during transit, and ensuring resilient operational protocols, are essential to protect against cyber threats and physical attacks. By addressing these security concerns, eVTOL cargo delivery systems can operate effectively and reliably, contributing to a more efficient and secure logistics network.

Regulations

- Regulatory considerations are crucial for integrating advanced technologies in aerial systems, particularly with the advent of 5G-enabled autonomous drones. A collaborative approach among governmental agencies is essential to establish comprehensive regulations ensuring

[25] Becker, S. (2022). How 5G Drones are Changing the Face of Delivery? - Elsight. Elsight. https://www.elsight.com/blog/how-5g-drones-are-changing-the-face-of-delivery/

[26] Texeira, K. (2024). Revolutionizing Air Cargo: The Rise of Air One Cargo eVTOL. LinkedIn. https://www.linkedin.com/pulse/revolutionizing-air-cargo-rise-one-evtol-kalea-texeira-w82hc/

safety, security, and efficiency. The FAA and USDOT must work closely to develop guidelines governing these aerial systems, addressing airspace management, safety standards, and operational protocols to facilitate widespread drone adoption. According to the FAA, measures have been finalized with the aviation industry and wireless providers to ensure that new wireless telecommunications systems can coexist with flight operations until at least January 1, 2028, mitigating the risk of 5G interference. Coordination with the FCC is vital to address spectrum allocation for reliable drone communication and data transmission. Additionally, DHS plays a key role in establishing cybersecurity standards to protect these systems. By working together, these agencies can create a regulatory framework that supports innovation while maintaining public safety and security.

Privacy Concerns

- The increased deployment of aerial systems, such as drones and autonomous aerial vehicles, raises significant privacy concerns related to data collection and surveillance. According to Nokia (n.d)[27], 5G networks exacerbate these concerns due to their ability to precisely track user locations with numerous antennas, posing risks from data leaks and attacks. Identity protection is further challenged by IMSI catching, which reveals communication patterns. The collection and storage of personal data by apps, combined with 5G's cloud-based storage, complicate data security, especially given differing global privacy standards. As aerial systems become more prevalent, they can capture vast amounts of data, including images and videos of individuals and private properties, raising critical questions about data collection, storage, usage, and access. The potential for misuse of aerial surveillance necessitates stringent regulations to safeguard personal information. Regulatory frameworks must address these issues by setting clear guidelines on data collection practices, ensuring transparency in data handling, and implementing measures to protect privacy. Regulations should define permissible aerial surveillance boundaries and establish protocols for securing and anonymizing collected data. By proactively addressing these privacy concerns, regulators can balance the benefits of advanced aerial technologies with individuals' fundamental rights.

Emerging Technologies to Potentially Investigate for Phase II

- **Digital Twins, Simulation, AR/VR**
    - Emerging technologies like digital twins, simulation, and augmented/virtual reality (AR/VR) offer new ways to enhance vehicle and infrastructure systems.
        - **Geofencing:** Geofencing technologies can improve traffic management and safety by creating virtual boundaries for vehicles.
        - **Testing of New Technology Systems:** Facilities like SunTrax provide controlled environments for testing new vehicle and infrastructure technologies. Red-team and cybersecurity testing are essential to identify and mitigate vulnerabilities.
        - **Access Control:** Digital means of access control can bridge the gap between cyber and physical security, enhancing overall system protection.
- **Artificial Intelligence (AI)**
    - AI technologies extend beyond individual vehicle applications to influence entire transportation systems.

[27] Nokia. (n.d.). Privacy challenges and security solutions for 5G networks. https://www.nokia.com/thought-leadership/articles/privacy-challenges-security-solutions-5g-

        - **Traffic Operations:** AI can optimize traffic operations and improve overall efficiency. However, ethical considerations and cybersecurity implications must be addressed.
        - **Data Mining and Prediction Algorithms:** AI-driven data mining and prediction algorithms can enhance city planning and transportation engineering by feeding digital twins and simulation models.
        - **Impact on Jobs and Workforce:** The deployment of AI technologies in transportation presents opportunities to augment local government capabilities but also raises concerns about job displacement.
- **Corporate/Physical Security Planning**
    - Defining corporate security holistically to include the implications of connected technologies is essential. Bridging terminology differences between public and private sectors can enhance understanding and collaboration in addressing security challenges.

Conclusion:

The integration of 5G technology into vehicles and highway infrastructure marks a transformative era in transportation, offering immense potential for enhanced connectivity, real-time data exchange, and improved traffic management. However, this advancement also introduces significant challenges, particularly in terms of cybersecurity, privacy, and regulatory compliance.

Our research highlights the critical importance of addressing wireless attacks as the primary threat vector to 5G networks and connected vehicles. The implications of these attacks range from critical sensor errors and navigation failures to potential national security threats, underscoring the need for robust cybersecurity measures. Additionally, the complexity of today's vehicle operating systems and the increased deployment of aerial systems like drones and eVTOLs raise further concerns about data security and privacy.

The success of 5G-enabled transportation systems depends on a comprehensive and collaborative approach involving both government and private sectors. Government agencies must develop and enforce uniform regulatory frameworks, facilitate public-private partnerships, and invest in advanced security measures. Meanwhile, the private sector should integrate security from the outset, enhance threat intelligence and detection capabilities, and promote interoperability and standardization.

As we look to the future, the ongoing development of advanced technologies, including AI, digital twins, and mixed reality, will further shape the transportation landscape. Addressing the associated risks and leveraging these innovations responsibly will be crucial for creating a resilient and secure transportation infrastructure.

In summary, while the integration of 5G technology presents numerous opportunities for revolutionizing transportation, it also demands a proactive and coordinated effort to mitigate risks and safeguard public safety. By fostering collaboration, implementing stringent security measures, and maintaining regulatory oversight, we can harness the full potential of 5G technology to build a smarter, safer, and more efficient transportation system for the future.

Appendix: Abbreviations

- ACARS: Aircraft Communications Addressing and Reporting System
- AEP: Analytic Exchange Program
- AES: Advanced Encryption Standard
- AI: Artificial Intelligence
- AR: Augmented Reality
- BVLOS: Beyond Visual Line of Sight
- CISA: Cybersecurity and Infrastructure Security Agency
- DHS: Department of Homeland Security
- DOT: Department of Transportation
- eVTOL: Electric vertical take-off and landing
- EU: European Union
- EV: Electric Vehicle
- FAA: Federal Aviation Administration
- FCC: Federal Communications Commission
- FDOT: Florida Department of Transportation
- FIRSTNET: First Responder Network Authority
- FMVSS: Federal Motor Vehicle Safety Standards
- HIDS: Host-based Intrusion Detection Systems
- IC: Intelligence Community
- ICT: Information and Communications Technology
- IDPS: Intrusion Detection and Prevention Systems
- IMSI: International Mobile Subscriber Identity
- ISO: International Organization for Standardization

- LOS: Line of Sight
- MFA: Multi-Factor Authentication
- NHTSA: National Highway Traffic Safety Administration
- NIDS: Network-based Intrusion Detection Systems
- NIST: National Institute of Standards and Technology
- NTIA: National Telecommunications and Information Administration
- PKI: Public Key Infrastructure
- PQC: Post-Quantum Cryptography
- RF: Radio Frequency
- SAE: Society of Automotive Engineers
- SBOM: Software Bill of Materials
- SCRM: Supply Chain Risk Management
- SDL: Secure Development Lifecycle
- SDN: Software-Defined Networking
- SQL: Structured Query Language
- STEM: Science, Technology, Engineering, and Mathematics
- TLS: Transport Layer Security
- UAM: Urban Air Mobility
- UAV: Unmanned Aerial Vehicle
- UN: United Nations
- UNECE: United Nations Economic Commission for Europe
- USDOT: United States Department of Transportation
- VR: Virtual Reality