The transportation system is rapidly evolving with new connected and automated vehicle (CAV) technologies that integrate CAVs with other vehicles and roadside infrastructure in a cyberphysical system (CPS). Through connectivity, CAVs affect their environments and vice versa, increasing the size of the cyberattack surface and the risk of exploitation of security vulnerabilities by malicious actors. Thus, greater understanding of potential -CAV-CPS cyberattacks and of ways to prevent them is a high priority.

In this article we describe CAV-CPS cyberattack surfaces and security vulnerabilities, and outline potential cyberattack detection and mitigation strategies. We examine emerging technologies—artificial intelligence, software-defined networks, network function virtualization, edge computing, information-centric and virtual dispersive networking, fifth generation (5G) cellular networks, blockchain technology, and quantum and postquantum cryptography—as potential solutions aiding in securing CAVs and transportation infrastructure against existing and future cyberattacks.

CAVs are the subject of research and development by both academia and industry because of their potential to improve traffic safety and operations. The limitations of human perception prevent motorists from discerning what is beyond the range of human sight, such as roadway incidents and work zones around a corner or in the far distance. Even autonomous vehicles' sensors fail to discern many such impediments. Vehicle-to-everything (V2X) communication provides a 360-degree view that transcends the limited capabilities of both human-driven and automated vehicles.

CAVs are planned to be part of a broader con-nected city initiative, communicating with other CAVs and with smart infrastructure and services.

CAV-CPS will use connectivity to improve roadway opera-tional efficiency using real-time roadway traffic information (e.g., about traffic signal phasing and timing, traffic incidents and queues) while improving safety in numerous ways, such as redundancy in case an automated vehicle's onboard sensors fail.

however, the highly interconnected CAV-CPS will introduce challenging security issues and vulnerabilities.

with far-reaching consequences for a poorly secured system. For example, attackers could gain access to CAV control systems and cause catastrophic multivehicle crashes. Thus, it

is critical to develop security solutions to protect CAVs, their occupants, other road users, and the associated infrastructure.

The Society of Automotive Engineers has created a cybersecurity guidebook of recommended practice, SAE J3061, that establishes a common terminology for security threats, vulnerabilities, and risks across the vehicular CPS (SAE 2016). SAE J3061 recommended practices are based on ISO 26262, an established standard for automotive functional safety (ISO 2018). The rapid evolution of CAV technologies requires adapting these standards and developing new ones to address CAV-CPS security challenges.

AV Security Vulnerabilities and Solutions

We divide CAV-CPS cyberattack surfaces into three main groups—

- in-vehicle systems, which include sensors, software, and in-vehicle network;
- V2X communication networks; and
- supporting digital infrastructure—

and outline countermeasures to cyberattacks in each category.

In-Vehicle Systems

Given the fatal consequences that may result if a CAV's in-vehicle systems are compromised, ensuring their security is of paramount importance to the automotive industry.

References: https://www.nae.edu/216540/Security-of-Connected-and-Automated-Vehicles