References

https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

What Is Vehicle Cybersecurity?

Today, cybersecurity affects each one of us on a multitude of levels. Our professional work, our personal lives—even our vehicles—depend on connectivity and technology that runs on complex software. As information technology becomes increasingly integral to our daily lives, our dependency on subsequent information systems grows. In turn, we experience an increase in vulnerabilities and potential attacks against those systems. Cybersecurity rose out of necessity to protect these systems and the information contained within them. Applied to vehicles, cybersecurity takes on an even more important role: systems and components that govern safety must be protected from harmful attacks, unauthorized access, damage, or anything else that might interfere with safety functions.

Increasingly, today's vehicles feature driver assistance technologies, such as forward collision warning, automatic emergency braking, and vehicle safety communications. In the future, the deployment of driver assistance technologies may result in avoiding crashes altogether, particularly crashes attributed to human drivers' choices. Given the potential safety benefits these innovations enable, NHTSA is exploring the full spectrum of its tools and resources to ensure these technologies are deployed safely, expeditiously, and effectively, taking steps to address the challenges they pose, including cybersecurity.

To ensure a comprehensive cybersecurity environment, NHTSA has adopted a multi-faceted research approach that leverages the National Institute of Standards and Technology Cybersecurity Framework and encourages industry to adopt practices that improve the cybersecurity posture of their vehicles in the United States. NHTSA's goal is to collaborate with the automotive industry to proactively

address vehicle cybersecurity challenges, and to continuously seek methods to mitigate associated safety risks.

Cybersecurity Protection Methods

NHTSA promotes a multi-layered approach to cybersecurity by focusing on a vehicle's entry points, both wireless and wired, which could be potentially vulnerable to a cyberattack. A layered approach to vehicle cybersecurity reduces the possibility of a successful vehicle cyber-attack, and mitigates the potential consequences of a successful intrusion. A comprehensive and systematic approach to developing layered cybersecurity protections for vehicles includes the following:

1. A risk-based prioritized identification and protection process for safety-critical vehicle control systems;
2. Timely detection and rapid response to potential vehicle cybersecurity incidents on America's roads;
3. Architectures, methods, and measures that design-in cyber resiliency and facilitate rapid recovery from incidents when they occur; and
4. Methods for effective intelligence and information sharing across the industry to facilitate quick adoption of industry-wide lessons learned. NHTSA encouraged the formation of Auto-ISAC, an industry environment emphasizing cybersecurity awareness and collaboration across the automotive industry.