Cybersecurity is a growing concern among vehicular manufacturers, transportation policy makers, drivers, and other third-party software service providers. Hackers, terrorist organizations, hostile intruders are possible attack vectors in exploiting communications causing sensor manipulation, disastrous collisions and traffic disruptions in vehicles. Today’s modern vehicles are well-advanced that each vehicle contains at least 80 or more processors, several in-vehicle networks, cables, I/O ports, and millions of lines of code. This combination of firmware increases the threat landscape. For example, according to Ford motors, F-150 Pickup truck has 150 Millions of Lines of Code in the overall architecture, which is higher than a modern Operating System or a Boeing 787. The following are challenges that hinders cyber security solutions:

- Limited external connectivity of the vehicle (Due to mobility)
- Limited Computational Performance (Due to high endurance and long-life cycle)
- Unpredictable attack scenarios and threats
- Hazard to drivers and passenger lives

This poster classifies the attack types and security properties in vehicular networks in three hierarchical layers: sensing, communication, and control layers.

**Multi-Layered Approach**

According to NHTSA (National Highway Traffic Safety Administration), a comprehensive, multi-layered and methodical approach is required to address the cyber security challenges. The following are some examples:

- A risk-based identification and protection process for safety-critical control systems is necessary.
- Timely detection and proper response to security threats on roads;
- Architectures, methods, and measures that improve resiliency of the system and facilitate rapid recovery when any incidents occur; and
- Methods of effective intelligence and data communications across the industry to enable quick adoption of industry-wide lessons learnt. NHTSA encouraged the formation of Auto-ISAC, an industry environment emphasizing cybersecurity awareness and collaboration across the automotive industry.