Executive Summary

As with many industries, the automotive sector is becoming increasingly dependent on computer technologies to provide the performance and differentiating features expected on its products. A few years ago, the automobile was mainly hardware and what happened in your vehicle typically stayed in your vehicle. That is no longer the case. The movement of digital innovations, from infotainment connectivity to over-the-air (OTA) software updates, is turning automobiles into software platforms.

Today's vehicles are increasingly 'connected'; there is wireless data exchange with servers, infrastructure, and other vehicles. Tomorrow's vehicles will be automated and autonomous, capable of sensing their environment and navigating through cities without human input. These advances will increase comfort and convenience for customers, improve products and services, and contribute towards achieving societal goals such as improving road safety, reducing fuel consumption, and facilitating traffic management and parking.

OEMs around the world are competing to integrate the most up-to-date features emerging from the consumer electronics industry as well as connectivity solutions that enable valuable remote services.

Besides, vehicle manufacturers have found highly attractive revenue opportunities and priceless insights into actual vehicle usage. Groundbreaking ADAS and autonomous driving technologies are increasing the demand for a continuous connection from the vehicle's ECUs (Engine Control Unit) to a variety of cloud services that would help to improve advanced sensor processing and subsequent vehicle maneuvering strategy, accompanied with the possibility to distribute new software updates and other necessary content into every ECU or infotainment system.

In the same way that new technology enables convenience during driving, it also leads to certain risks if some precautions are not taken. Current advancements in functional safety evaluation and implementation of its corresponding elements in hardware and software (ISO 26262) during product development always guarantee a defined operating state for every safety-critical element (e.g. steering, braking, ADAS) within the vehicle. But all these efforts may be compromised if security features to protect the ECU software against unauthorized access and modifications are not implemented.

In times before wide-spread external connectivity solutions for cars, this deficiency did not pose a high risk as physical access to the vehicle communication was necessary to trigger commands that could result in serious threats to safety such as deactivation of the brakes, autopilot or steering system during driving.

However, today we have an automotive ecosystem that is much more complex due to the following factors:

- Steadily increasing penetration of connected vehicles worldwide
- Standardized vehicle platforms sharing the same electronic backbone
- Support for external connection of brought-in devices (wired and wireless)
- Integration of content and services provided by third parties
- Lack of hardware and software security elements in ECU designs

The relationship between customers and their vehicles is very personal as most drivers see their cars as an extension of their private space much like their homes. Consequently, unavailability of their vehicle caused by a large-scale security breach or a malfunction of safety components during driving would lead to a disruption of trust in the vehicle and its manufacturers.

The digital world offers unprecedented opportunities. Then come with high risks. The overall security of modern mobility services will depend on how well the industry addresses cyber-risks in and around connected cars, as well as on the strategic actions key players take today to prepare for future attacks.