INTERACTION BETWEEN VULNERABILITIES FOR THE AUTONOMOUS AND CONNECTED VEHICLES: PROCESS AUDITING

While autonomous and connected vehicles offer tremendous benefits, they also pose new cybersecurity and traffic safety challenges. The gap in the industry's ability to assess and manage these threats is widening. The threat landscape is dynamic and evolving rapidly, so traditional approaches are increasingly insufficient. A secure product considers the whole system, from sensors to the cloud. Over the course of this project, TÜV SÜD has used frameworks from ISO and general risk management concepts to develop a systematic and comprehensive approach to help develop highly secure and safe products.

MARKET FACTS AND OUTLOOK

Approximately 13 million highly automated vehicles were on the roads in 2015. The forecast amount will be 33 million in 2018 and 100 million in 2030. With autonomous and connected vehicles, information is exchanged with external road systems, such as traffic lights, streetlights, and cameras. This information exchange is bi-directional. Autonomous systems such as traffic lights, streetlights, and cameras will communicate with other autonomous systems. Autonomous and connected vehicles use telematics, in-vehicle software, and smart phones for data exchange to access cloud-based infrastructure. Malicious mobile apps and other attacks, such as Denial of Service, spoofing attacks, Denial of Service, and Advanced Persistent Threats, can compromise the security of vehicles and networks.

WHAT ARE THE POTENTIAL CONSEQUENCES OF CYBER ATTACKS?

- Loss of brake control
- Loss of steering control
- Loss of engine control
- Manipulated navigation
- Malicious mobile apps
- Inoperative lights
- Disrupted passenger safety systems
- Infrastructure data
- Personal data
- Revenue loss
- Brand damage
- Commercial loss
- Data theft
- Vehicle systems fail
- Takeover control
- Driver injuries or deaths
- Pedestrian injuries or deaths
- Faulty diagnostics
- Vehicle theft
- Collison

HOW WILL AUTONOMOUS VEHICLES COMMUNICATE?

Vehicle-to-Vehicle (V2V) interactions allow vehicles to exchange real-time information about positions and speeds. Vehicle-to-Infrastructure (V2I) interactions enable vehicles to exchange information with traffic lights, streetlights, and cameras. Vehicle-to-Network (V2N) interactions allow vehicles to connect to external cloud infrastructure. Software updates and diagnoses can be done wirelessly.

HOW CAN TÜV SÜD HELP YOU?

TÜV SÜD is developing reliable testing methods and standards for the safety and cyber security of autonomous and connected vehicles. This includes participation in standardisation committees to develop appropriate global regulations and assessment of safe and secure development. TÜV SÜD is also responsible for the development of new features, data flows, and new functionalities such as traffic light control, parking assistance, and smart parking.