Securing connected cars

Continental has introduced its security strategy, which includes to check continuously the communication on the CAN-based in-vehicle networks.

The end-to-end security solution enables to detect as soon as possible attackers (Photo: Continental)

Functions such as wireless updates to vehicle electronics are accompanied by risks. The further interconnectivity goes, the more demanding the requirements become on general security specifications and standardized frameworks. That is why cyber security is at the heart of the development of products and services at Continental. The company is developing end-to-end solutions with the aim of ensuring a high degree of security. "Until now, most reports of vehicle hacks have been attributed to security researchers or ‘white hat’ hackers. To ensure that nothing changes in that respect, cyber security needs to be taken into account right from day one in product development, so that potential security loopholes do not arise in the first place," said Andreas Wolf from Continental.

To ensure that the complex vehicle system and all its individual components can be reliably secured, Continental has chosen a multi-layered approach. This involves conducting a detailed risk analysis for new projects to ensure secure products and services that comply with the regulations. "We refer to this process as 'security and privacy threat analysis, risk assessment and risk treatment', and we consider not only initial development but also the entire product life cycle," explained Wolf.

In addition, end-to-end security solutions are used with the primary goal of detecting and preventing attacks on a vehicle (external interface protection & monitoring). To do this, the German supplier protects the vehicle's communication interfaces with the outside world. The vehicle system itself also needs protecting. One method of doing this is to constantly check communication on the CAN-based in-vehicle networks for anomalies, and for communication between individual control units to be encrypted (in-vehicle network protection & monitoring). One significant aspect that the company also takes into account in its approach to security is that of permanently monitoring the current status of the vehicle system (in-vehicle state-of-health monitoring). This must be reported regularly to a security operations center, such as the one operated centrally by Continental, so that vehicle fleets in the field can be checked for security loopholes. In serious cases, automotive manufacturers and suppliers can thus look for solutions, develop a security patch and update the vehicle fleet via over-the-air updates without the need for a workshop visit, all within a short space of time.

"We are building up an entire ecosystem of security-relevant elements for our solutions so that we can offer our customers a customized design from a single source, and one that is available right from the early definition phase of a project," said Wolf. The overall package is completed by the involvement of software products of the Continental subsidiary Elektrobit. This enables the developers to call upon both basic software components and application software when building the security architecture for the electronic control units so that they can make the system secure.

Cyber security is one of the major tasks facing the entire automotive industry when it comes to the connected car of the future. Continental looks at it from four angles. The first concerns the individual electronic components, which act as tiny computers responsible for all manner of functions in the vehicle, from the engine control unit to the windshield wipers and the access control system. Secondly, the communication between these individual parts is observed. Thirdly, the numerous interfaces between the vehicle and the outside world need to be protected. Fourthly, with the car as part of the Internet of Everything, cyber security needs to be considered beyond the limits of vehicles, including the cloud and the back end as well. "It is clear that absolute security is not possible. Industry will always be racing against cybercriminals. With our solutions, however, we are creating state-of-the-art barriers against cyber-attacks and making them as high as possible."

hz