Preview ATZelektronik 07.-08.2024

COVER STORY | SECURITY

Security is based on the software-side integrity of complete product and company security: if there is one place where end-to-end thinking counts, it is in protecting against cyber attacks. As no company wants to risk an attack from the inside, security must be considered and designed comprehensively and not just product-centred. This applies in particular to high-priced, highly complex and, in terms of driving dynamics, dangerous objects such as vehicles. The fact that there is no such thing as absolute and, above all, permanent safety must be accepted as a given. It therefore stands to reason that, in addition to ensuring that vehicles and their cloud infrastructure are as secure as possible, emphasis must be placed on effective, rapid proactive responses.
Consequently, if OEMs were to use their own proprietary software stacks, they would either have to set up their own security departments similar to those of large software providers in order to be able to roll out bug fixes quickly - or purchase this service from specialised companies. Both options will not necessarily be cheap, but are essential to ensure the secure functioning of tomorrow's vehicles.

The post-quantum calculation
Information technology is on the threshold of the quantum age. This is not good news for the cyber security of future vehicles and their networked systems, as today's security mechanisms will be defeated by quantum computers. The article shows how benchmarks for quantum-safe automotive security procedures are being developed. Etas

Cybersecurity in the automotive industry: upcoming risks and new insights
New vulnerabilities in software-defined vehicles, such as storage and management of cloud-based of cloud-based data offer attractive targets for cyber attackers. The article describes, how cyber threats are proportional to the development of software defined vehicles and the integration of new technologies such as artificial intelligence. VicOne

Countering security threats with root-of-trust methods
Today, electronic systems in automotive products are inevitably a target for cyberattacks. Over the past 10 years, OEMs, their suppliers and semiconductor manufacturers have made considerable efforts to implement various security technologies, including hardware-based ones. The article shows which security threats should be prioritised and how existing security measures can be improved to ultimately reduce the risks of hacker attacks using root-of-trust approaches. Renesas

IN FOCUS

Micromobility - more than just a toy
Micromobility is set to change the urban landscape. For a few years now, the new electric scooters in particular have been causing a stir - both positively and negatively. On their routes, they are competing with the traditional bicycle or the cargo bike, which has also entered the picture

HANSEN REPORT

As a source for technology and business trends in the global automotive electronics industry, Paul Hansen highlights current industry topics within the framework of ATZelectronics resp. ATZelectronics worldwide, Paul Hansen highlights current industry topics.

Dates

Advertising deadline: 06/21/2024
Copy deadline: 06/27/2024
Publication date: 07/19/2024

Contact

Rouwen Bastian
Sales Management
+49 (0) 611.7878 399
rouwen.bastian(at)springernature.com