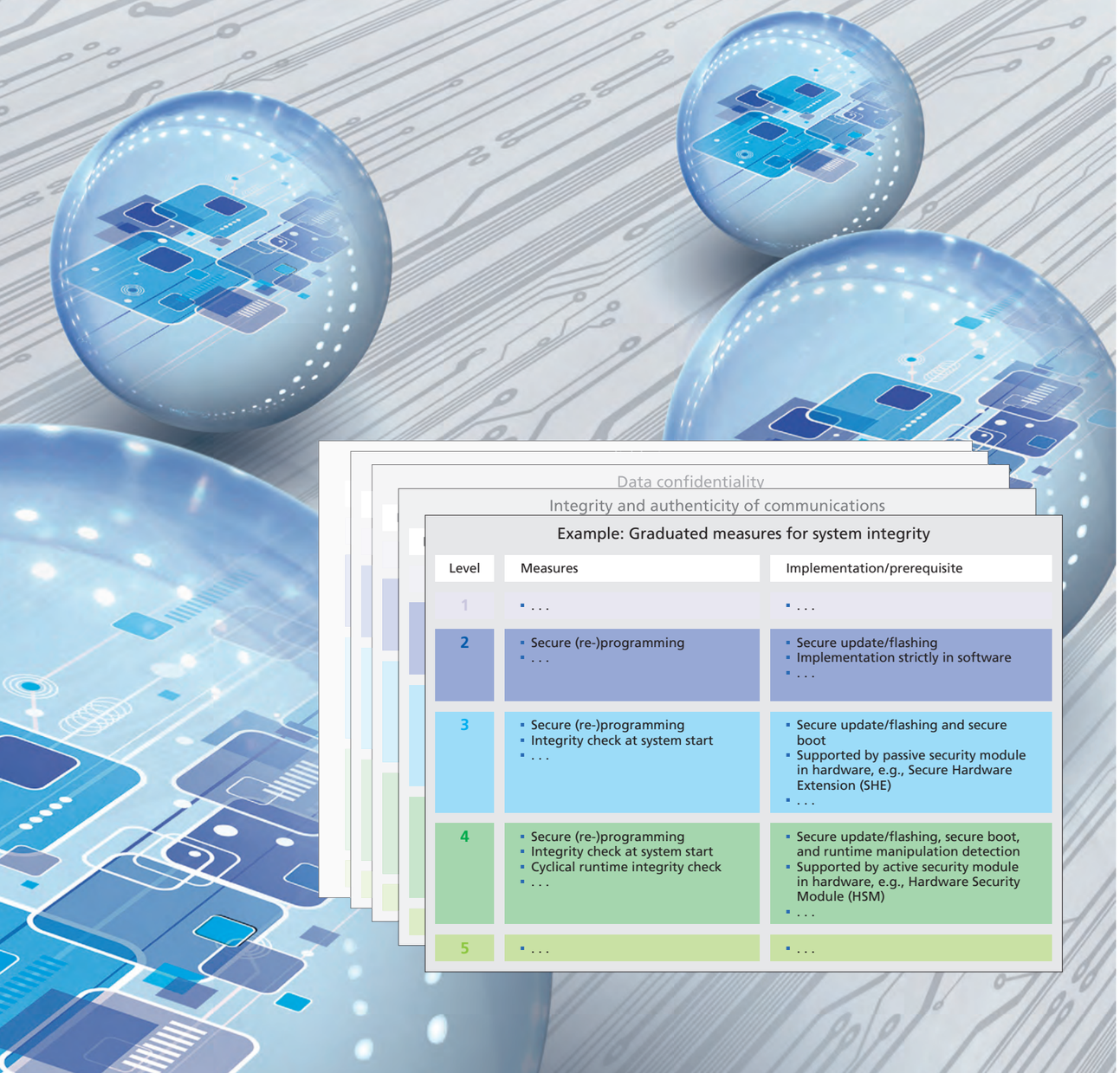
Safety and Security – A Holistic Approach



Connected vehicles require new risk awareness

IT systems in the vehicle are becoming more accessible to the outside world. This brings new opportunities, but also new risks, which calls for a fundamental reevaluation of risk assessment and security architecture. Safety and security will have to mesh more tightly in the future. What is needed is a holistic approach that encompasses all components of the vehicle throughout its entire life cycle.

A sonorous voice points out tourist attractions, provides historical background information, and occasionally mentions current offers from local bars and shops. You're taking an online city tour in your own car, using an advertising-funded program based on connected technologies. Sensors monitor the surroundings and transmit this data to ECUs and the communications unit in the vehicle, which maintains contact with the traffic control center and other vehicles in the vicinity.

Thanks to this ongoing exchange of data, traffic keeps moving. Accidents and jams are a rare occurrence. Traffic lights use incoming vehicle data to adjust their cycles to the traffic volume in real time, which reduces the level of CO_2 emissions from road traffic. Vehicles searching for a parking space no longer disrupt the flow of traffic. Drivers and passengers get out of their cars in designated stopping zones, and web-based systems proceed to guide their vehicles to the next available parking space. The automatic parking assistant can calculate the parking maneuver required in advance by evaluating the data of the car that was parked there previously.

Vulnerabilities have no place in a successful network

This vision of the future only suggests the potential of connected transport. No one knows what business model options will open up when vehicle IT systems that used to be closed off to the outside world are connected as parts of larger networks. Upgraded engine performance, navigation and assistance systems are just as conceivable in the "internet on wheels" as reduced insurance rates based on voluntarily submitted driving data. However, opening up data channels for apps, upgrades, and any mobile devices from various occupants of the vehicle or Car-to-X data traffic brings new and, in part, unknown risks in the development stage. Minimizing these risks requires a fundamental reevaluation of risk assessment and security architecture.

Despite opening up more to the outside world, intrinsic security remains the goal. Under no circumstances should hackers or viruses smuggled in via mobile devices affect the safety of the vehicle and its occupants. The vehicle should also be automatically protected against the unwarranted installation of untested software by unauthorized providers without the driver having to do anything. Protection must therefore be integral to the vehicle's IT architecture.

Risk analysis and assessment throughout the entire life cycle

Clearly, a technological shift is called for: Security, defending against external attacks, and safety, ensuring that system functions don't fail in the event of an emergency, will have to mesh more tightly in networked vehicles than has been the case up to now. Security and safety experts should put their heads together before software and hardware development has even begun in order to identify and evaluate potential risks.

They could then formulate risk objectives using assessment procedures that rate the probabilities and consequences of potential disturbances in line with the ASIL scale in the ISO 26262. This fundamental analysis follows a holistic approach, and should take into account permanently installed components as well as intermittently connected smartphones, service diagnostics devices, servers, and vehicles exchanging data over-the-air (OTA).

Once the risks within the system have been assessed and the safety and security requirements identified, the software architecture can be designed. Even at this early stage, the engineers must clarify

In a networked world,
secure systems require comprehensive protection.

AUTHORS

Dr. Simon Burton is Director Global Embedded Software Services at **ETAS GmbH**.

Dr. Martin Emele is Head of the Product Security Group at **ETAS GmbH**.

Dr. Thomas Wollinger is Managing Director of **ESCRYPT GmbH.**

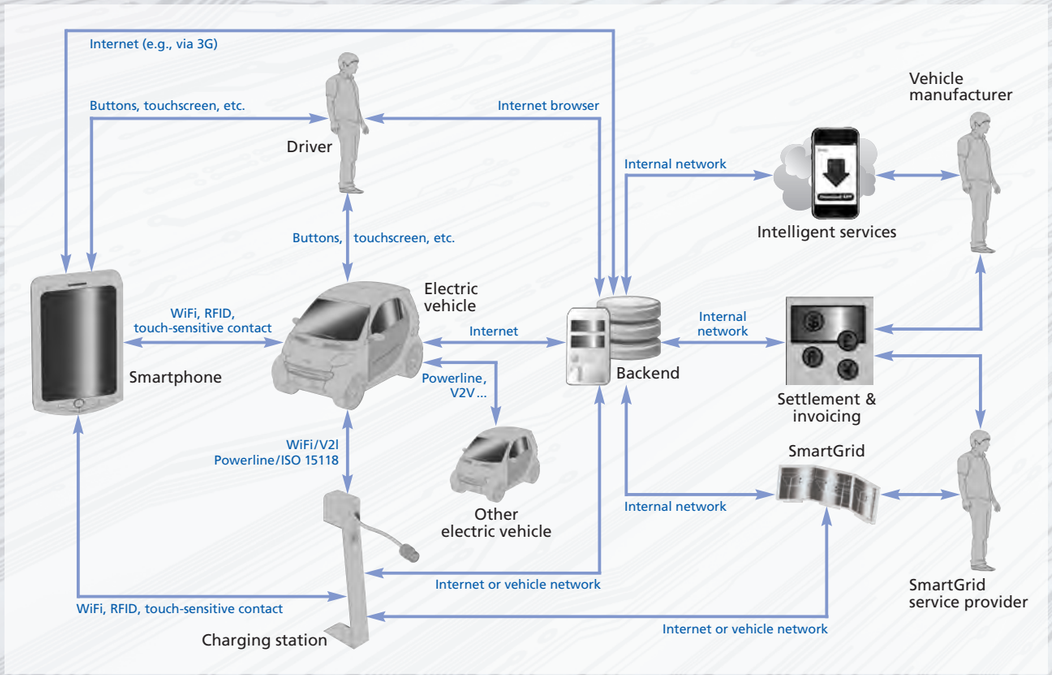
which data will go in the ECUs and how they will get there, who is allowed to read and/or change specific data, and which specifications subsequent functions and tests will follow. As connectivity increases, the deciding factor is that, once they have been delivered, vehicle systems are open to interaction with the complex outside world.
Remote access privileges for service workshops must be clarified, and senders of incoming data authenticated. Cryptographic data must also be protected against unauthorized access – from the start of development right through to their disposal. When no longer required, the vehicle's unique cryptographic keys must be reliably deleted to prevent security-relevant information getting into the wrong hands.

An overview of all components

Other sources of risk include over-the-air firmware and software upgrades (FOTA/SOTA) and apps that intervene in the vehicle software. Their intensified interaction with controllers, sensors, and actuators poses a threat to the overall network. The magnitude of this threat has been shown in experiments in which developers were commissioned to hack their way into vehicle functions from the outside.

In 2015, for instance, a team in the United States succeeded in actuating the brakes and stopping the engine in a moving test vehicle, albeit with great effort. Manufacturers must take precautions against such attacks; for example, by protecting each vehicle with firewalls, gateways, and secured communication with unique cryptographic keys. Secure key management has a threefold effect: If every vehicle is protected by unique cryptographic keys, hacker attacks become much more difficult and, in the worst case, only affect a single vehicle. Moreover, the requirement to authenticate fulfills a gatekeeper function against unknown software and their senders.

The connected vehicle networks of the future provide numerous interfaces.



Data exchange only with authenticated partners

In the future, professionally installed security solutions backed by secure data centers staffed by appropriately qualified associates will determine participation in Vehicle-to-X communication. Data will only be delivered to the recipient if the sender can provide a trusted signature. Cross-manufacturer and cross-sector key management solutions also help vehicles to filter out relevant information from the flood of data.

Establishing security solutions will therefore become mandatory for all stakeholders in connected traffic. In the event of an emergency, however, safety solutions must also take effect. Systematic engineering geared towards standards such as the ISO 26262 ensures that all important vehicle functions remain operational even in the case of attack or negligent viral contamination.
Consequently, it is important that security-relevant areas are reliably safeguarded against the effects of software installed at a later date. Commercially available solutions include ETAS' Hypervisor RTA-HVR, which partitions a single ECU into multiple virtual ECUs that are strictly separated from each other, thereby completely shielded the ECU's functions from outside influences. This method requires core functions in need of protection to be defined in advance. Given the intense interaction that takes place between ECUs in the vehicle, this requires a great deal of experience, a tried-and-tested methodology, and efficient tools. These might include Software- and Hardware-in-the-Loop testing facilities, functional security protocols, or the equipment required to carry out real-time monitoring of memory accesses, computing times, and transfer rates. Last but not least, the process calls for skilled associates who are comfortable working in this development environment, and who are familiar with the required norms and industry standards such as AUTOSAR.

Utilizing existing knowledge

Customers will find all of this at ETAS. Our modular product and service portfolio starts with expertise and many years of experience in the planning, implementation and testing of secure embedded software, and continues with AUTOSAR-compliant operating systems and protocols for secure communication, and goes beyond tools such as our Hardware Security Module (HSM) or the Hypervisor RTA-HVR mentioned above.
Manufacturers will soon be able to use the latter to reserve selected areas of ECUs for their own updates and upgrades. This is yet another way to guarantee a bit more safety and security in the future connectivity market. Also available are the modular security solutions provided by ETAS subsidiary ESCRYPT, which extend across the entire life cycle of all new vehicles and cover cryptography software licenses through to complete key management, inclusive of processing in top-security data centers.

Applying know-how for affordable risk minimization

Cost reasons alone render the complete compartmentalization of every ECU in connected vehicles impossible. Compromises are necessary that can only be made on the basis of risk analysis and assessment, which makes an all-encompassing view of the safety concept for all vehicle systems essential. Should, in the worst case the security and safety of a function be particularly threathened, routines can be implemented to react accordingly, all the way up to a coordinated shutdown of the system.

Systematically interlinking security and safety approaches is crucial, because future threats are not yet known. The only effective means of equipping connected vehicles to face these unknown risks is to combine suitable key management with secure vehicle system design. It is not enough simply to respond to threats as they materialize. Fundamental flaws in security architecture cannot be fixed via an update, and, given the limitations of restricted data transfer rates, annoying security updates should be kept to an absolute minimum in any case.

Summary:
Adjust risk awareness – assemble a package of measures

Networks of connected vehicles require new risk awareness. The huge number of vehicles, the frequency with which they are used, and their connection to external data streams increases the likelihood of disturbances. To minimize the resultant damage, safety and security solutions that usually operated in isolation must now become much more interlinked. A holistic overall assessment of the risks prior to development is an essential prerequisite to reliably safeguard connected vehicles against current and future risks. "Safe and secure by design" should be the motto throughout the entire product life cycle.