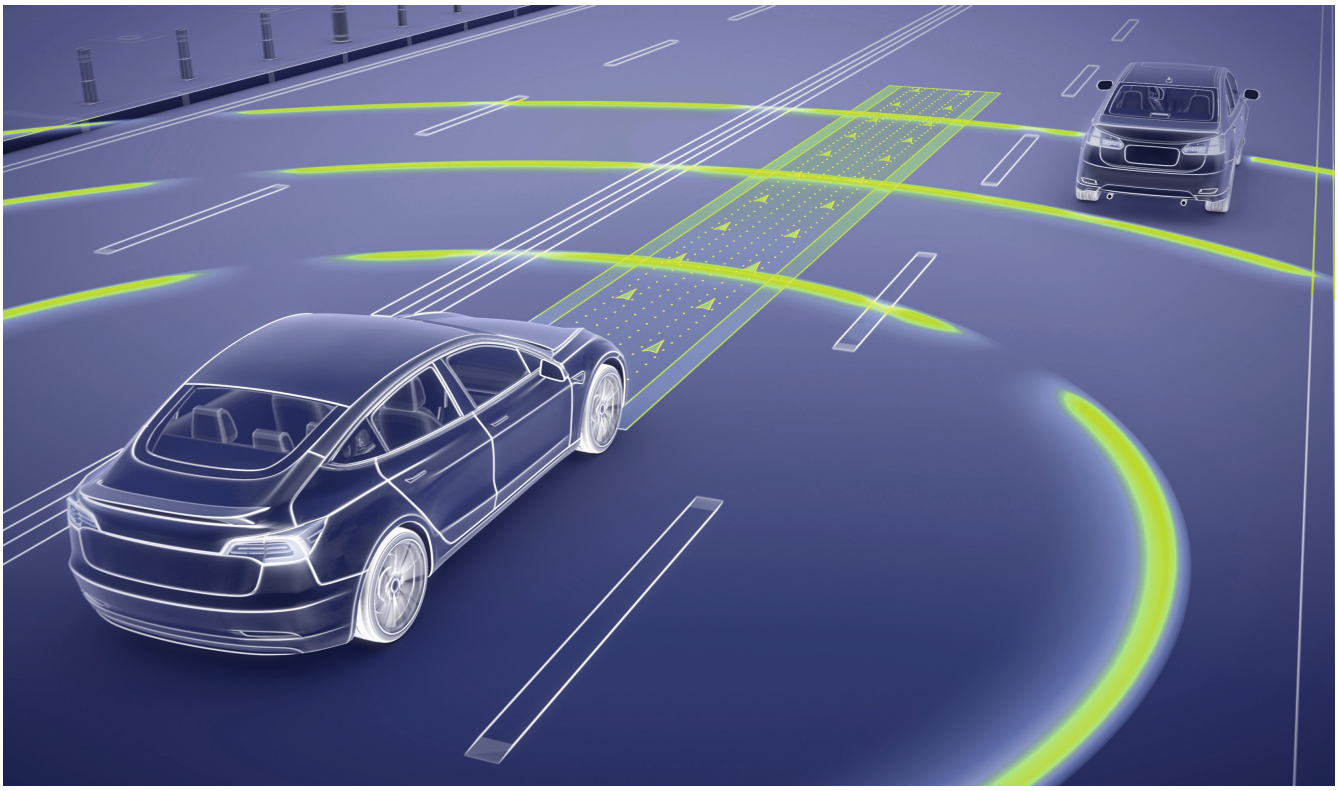


Automated driving: No safety without security

05 APR 2019 NEWS

Automated driving systems are designed to make driving safer and more comfortable. However, the increasing connectivity of safety-relevant functions and the integration of new technologies into vehicles pose new challenges for IT security. The use of Ethernet for in-vehicle communication enables much higher payloads and transmission rates, and the integration of powerful microprocessors offers higher performance. However, both of these technologies are well-known in the traditional world of IT, with attack vectors familiar to hackers. The use of such technologies in vehicles, especially in their safety-relevant functions, therefore calls for suitable security measures that prevent both known attack patterns and new types of attacks.

The E/E architecture in automated vehicles differs significantly from traditional IT in terms of what it is designed to protect: the prevention of human injury and machine damage is top priority here. That is why the authenticity of the network traffic and the availability of the connected systems have absolute priority. Nonetheless, privacy must not be ignored, especially in the case of data from

automated driving systems that can be linked back to individuals and thus falls under the data protection legislation. So automated driving requires a secure connection to external systems alongside a clear separation between external and internal networks. At the same time, in-vehicle communication via Ethernet as well as via conventional vehicle buses must be securely implemented within an E/E architecture – all the while taking into account the special requirements concerning security, safety, and reliable time response.

Security measures in modern E/E architectures

When using existing domains based on virtual networks (VLANs), the virtual zones are separated in accordance with their need for protection: the network traffic of security-relevant components in real time must be prioritized over and isolated from other systems. If, for example, the network is flooded with packets due to a component malfunction or a denial of service attack, rate limiting can be applied to restrict this traffic at the next switch. This allows communication to continue in the prioritized VLAN, with safe operation of the vehicle guaranteed.

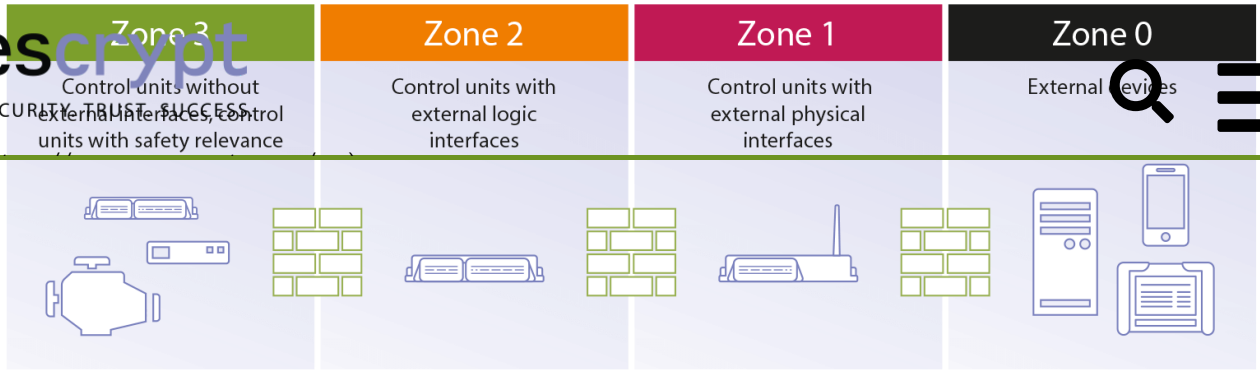
Firewalls are another feature that can be used to secure E/E architecture and in-vehicle communication. They use filter rules to control the permitted exchange of data between different networks or endpoints. Modern automotive firewalls are also able to analyze and evaluate communication right down to the user data level using deep packet inspection. Building on this, intrusion detection systems (IDS) and intrusion prevention systems (IPS) (https://www.escrypt.com/en/solutions/Intrusion-detection-and-prevention-for-vehicles) can be implemented to detect and prevent unauthorized data traffic in the network.

That said, the logical separation of network traffic is no substitute for cryptographic authentication or encryption and, as such, does not fully protect against unauthorized access. There is, however, a software module that can help here, called Secure Onboard Communication (SecOC) for AUTOSAR. In addition, the adaptation of traditional Ethernet security mechanisms such as (Datagram) Transport Layer Security ((D)TLS), IPsec, and MACsec (IEEE 802.1AE) provides basic protection of automotive Ethernet communication against manipulation.

Designing a secure E/E architecture for automated driving

When designing an E/E architecture, is important to consider how to integrate established security measures efficiently and securely. The following four starting points must be taken into consideration when protecting against unauthorized access and isolating safety-relevant communication:

1. *Separating zones according to safety relevance*



(Architecture overview) https://www.escrypt.com/fileadmin/user_upload/images/ECSRYPT_Fachartikel-ATZextra_Zonen-EE-Architektur_Web_engl.jpg

The basis of a secure E/E architecture is a clearly defined classification and separation of the vehicle network into individual zones (such as domains, VLANs, and IP subnets) according to their safety relevance. At the same time, the number of dedicated ECUs with external interfaces should be kept to a minimum. Based on these two parameters (isolation of safety-relevant communication and minimization of external interfaces), ECUs can be assigned to specific zones and safety and security classified within the E/E architecture.

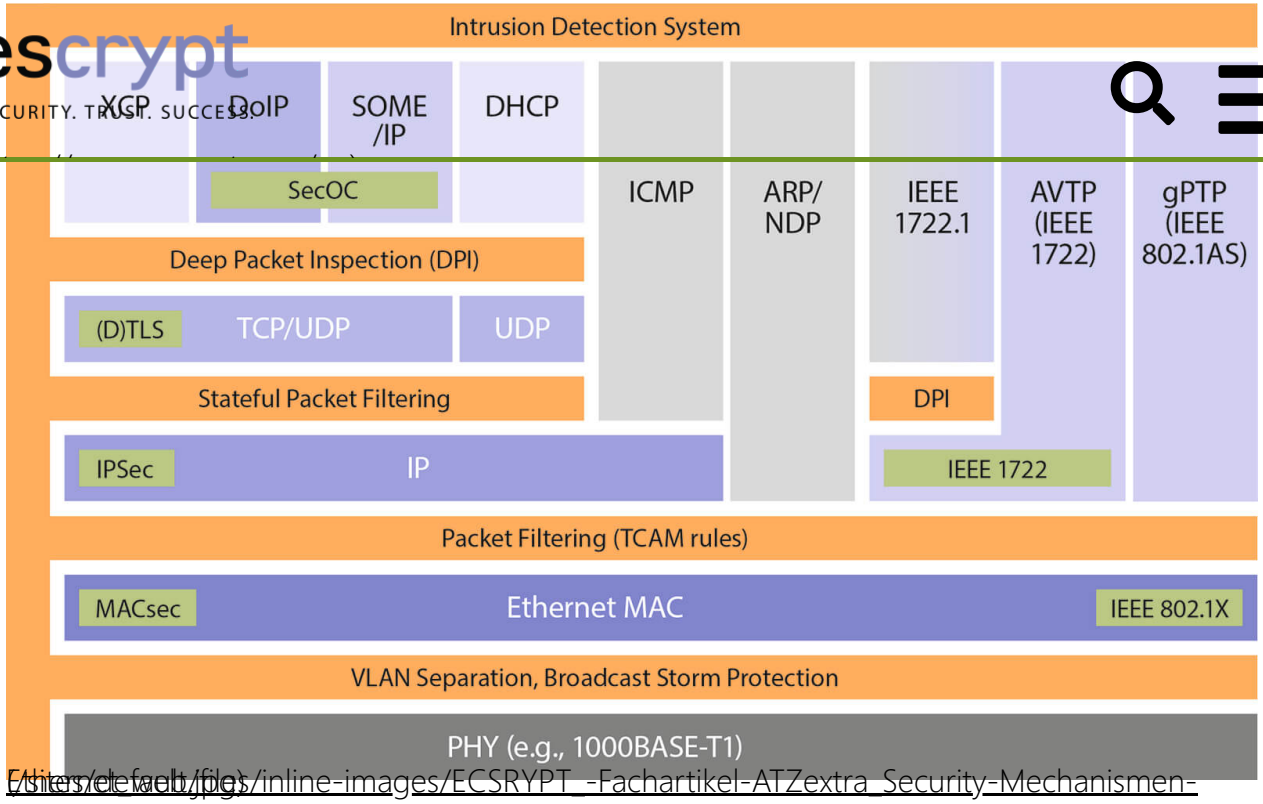
2. *Monitoring and controlling electrical system communications*

Firewalls and ID(P)S ensure that only legal and authorized data exchange can take place across domains or VLANs. Solutions are already available for in-vehicle use that can efficiently control and analyze the communication of traditional vehicle buses while also respecting the various Ethernet protocols across multiple network layers. Optimum use is made here of Ethernet switches' hardware mechanisms to enable even the higher protocol layers to be analyzed in real time.

3. *Securing the Ethernet switches*

The use of Ethernet switches in the E/E architecture and on ECUs is relatively new. This makes it all the more important to protect the switches against external manipulation when using security measures such as firewalls and ID(P)S. Integrity and authenticity must also be verified when programming and secure booting the Ethernet switch in order to prevent things like manipulation of the VLAN configuration or unauthorized changes to firewall rules. Furthermore, a specific switch configuration is necessary.

4. *Ensuring secure data transmission*



/sites/default/files/inline-images/ECSRYPT_-Fachartikel-ATZextra_Security-Mechanismen-

In traditional bus systems, SecOC can be used to prevent manipulation of messages that need to be protected; however, at this stage no encryption of data traffic is envisioned. In contrast to SecOC, Ethernet-based security protocols (e.g. (D)TLS, IPsec, and MACsec) ensure not only data authenticity and integrity but also data confidentiality. Since the protocols work on lower network layers, they are able to secure both signal-based communications over the Ethernet (such as User Datagram Protocol [UDP]) and the service-based communications (e.g. SOME/IP) used in automated driving. Given the strict real-time requirements in the vehicle, this involves implementing particularly fast, symmetrical procedures based on the use of pre-shared keys.

Developing and designing a secure E/E architecture forms the very basis of automated driving. And applying the right specialized security solutions can permanently guarantee the authenticity, integrity, and confidentiality of data and functions within the vehicle electrical system. Seen from this perspective, one thing is for sure when it comes to automated driving: if you want safety, you have to pay attention to security from the outset.

UNECE WP.29 and ISO/SAE 21434: Automotive cybersecurity faces new challenges (/en/news-events/unece-wp29_iso-sae-21434)

read more (/en/news-events/unece-wp29_iso-sae-21434)

escar Europe 2020 goes hybrid (/en/news-events/escar_2020_hybrid)

read more (/en/news-events/escar_2020_hybrid)

V
m
h
(/
w

ev

escrypt
SECURITY. TRUST. SUCCESS.

(https://twitter.com/escrypt)
(https://www.xing.com/companies/escryembeddedsecurity)
(https://www.linkedin.com/company/40trk=tyah&trkInfo=clickedVertical:compa1-1,tarId:1461659885814,tas:escrypt)
(https://www.youtube.com/channel/UC(
(https://weixin.qq.com/r/YkU_JjLEnm-hrXZF9xBw)

Publications

Research projects (/en/research)
Downloads (/en/downloads)
Terms and conditions (/en/terms_and_conditions)

Contacts

Newsletter

Subscribe to our monthly newsletter

Email address **subscribe**

Unsubscribe Newsletter

Language: English