“Cybersecurity is becoming a prerequisite for type approval”

Dr. Moritz Minzlaff on automotive security as a strategic task

Increasing security requirements for vehicles are manifesting themselves in a wave of new standards and regulations. In this interview, Dr. Moritz Minzlaff, Senior Manager at ESCRYPT in Berlin, explains what the automotive industry has to adapt to.

Mr. Minzlaff, efforts to create binding standards and regulations in the field of automotive security are now in full swing. Which developments deserve special attention here?
There are two initiatives that everyone is watching right now: first, ISO/SAE 21434, which sets standards at the process level; and second, the activities of UNECE WP.29, which will make cybersecurity a prerequisite for the type approval of vehicles. Both the UNECE regulations and the ISO specifications will come into force within the next three years. So there’s really not much time to prepare.

This means that in the near future the IT security for vehicles will truly be relevant for type approval!
That’s right. In the future, according to UNECE specifications, OEMs will be able to approve vehicle types in markets such as the EU or Japan only if they can demonstrate appropriate risk treatment. ISO/SAE 21434 will be the key to overcoming this hurdle by offering common security standards for the automotive industry. At the same time, further regulations and laws are constantly being developed at the regional level, which must also be kept in mind.

What are the specific challenges facing automakers and suppliers?
The big challenge is that in the future, security must be approached comprehensively right across the supply chain and life cycle. It is no longer enough to provide two or three central ECUs with security functions. Vehicle manufacturers will have to identify and secure critical elements for the entire platform – all the way through to phase-out. This means life cycle management will be a decisive topic in the future. In other words, how do you provide adequate risk-based protection after start of production for connected vehicles that face many years of exposure to a constantly changing threat landscape out on the road?

As an OEM or supplier, what should I do now to make vehicle protection a permanent fixture in my corporate actions and my organization?
You need to act on two fronts. First, you should determine the security requirements of your product: vehicles and components with different degrees of connectivity, different functionalities, different safety relevance, and different degrees of automated driving each require tailored protection. To achieve the security level identified in this way, you’ll need to involve all participants: from development and production through quality assurance to sales and customer communication, responsibilities and roles must be clearly defined within the company and along the supply chain.

At the same time, you can carry out an “inventory,” in other words a standard audit or assessment. Which areas are you well positioned in? Which aspects of future regulatory requirements do you already meet? And which existing processes can you build on? A gap analysis of this kind will point out where investments in the further development of security will have the greatest impact.

Does it make sense to get a security specialist like ESCRYPT on board?
Yes, because our independent perspective and our global, industry-wide know-how is the ideal complement to your in-house expertise. The only way to achieve continuous protection of connected vehicles is by working together and taking a holistic approach. That’s why, at ESCRYPT, we’ve already combined classic enterprise IT security with embedded security. Because the only way to master cybersecurity in the future is across domains, from vehicles to apps to clouds.

Dr. Moritz Minzlaff
Senior Manager at ESCRYPT

Due to our diverse project experience with manufacturers and suppliers in all major markets, we can also offer benchmarking. We identify exactly those aspects of security as currently practiced that should be further developed, and we help identify the necessary investments in cybersecurity. Time is short and the risk is too great not to achieve type approval according to UNECE specifications or to do so only with a delay or cost overrun. Thanks to our in-depth engineering experience, at the end of the day we at ESCRYPT know how to bring automotive security into series production. All this massively increases the chance of successfully mastering the challenges ahead. ■

"The only way to achieve continuous protection of connected vehicles is by working together and taking a holistic approach."