© Etas

"The security must be met as well as the modular commercial vehicle ecosystem supported"

System development in the software area is inextricably linked to the aspect of security. This applies to both the passenger car and the commercial vehicle (CV) sector. The CV segment differs in terms of greater modularity and more comprehensive cooperation between the manufacturers. The passenger car segment could learn a lesson in this and other aspects, says Dr. Jan Holle from Etas.

ATZelectronics_ Is there anything that distinguishes software development for commercial vehicles from that for passenger cars?
HOLLE _ There's certainly no answer that applies equally to all commercial vehicle manufacturers. We are delighted with the great pragmatism we are experiencing in our security software (SW) projects. In our observation, manufacturers clearly want to rely on highly reusable standard components and enjoy the resulting economic benefits. We're also seeing some very cooperative collaborative models, up to and including joint development of requirements and the corresponding software components.

What requirements does software development for commercial vehicles have to satisfy?
We see hardly any major differences between software development for commercial vehicles and for passenger cars when it comes to non-functional requirements, quality, and processes like MISRA, ASPICE et cetera. I would

say the biggest difference is how to develop software together and specify the right software packages. Commercial vehicle manufacturers are far more sensitive to initial software development costs and to potential maintenance and adaptation costs because of their comparable low production volumes. Looking at it from the security perspective, we're also seeing exciting special use cases such as platooning.

Is agile software development an option for commercial vehicles, too, or do classic methods dominate because cycles are slower?
Exactly as in the passenger car sector, there is a great deal of heterogeneity here. Some commercial vehicle manufacturers are already using agile software development methods, or are at least ready to engage with the agile methods we use, such as SAFe, the Scaled Agile Framework. Of course, there are also manufacturers who still tend more towards the classic methods. We are seeing some commercial vehicle manufacturers exhibit the kind of agility that in the passenger car sector we rather experience more with startups. This is perhaps explained by the relatively small size and simpler organizational structures of these enterprises. So progress is not necessarily slower, even if product cycles may be longer. By the way, we're also seeing the aforementioned heterogeneity in the level of organizations' maturity with regard to security. This heterogeneity requires tailored answers to achieve the requisite maturity level, for example, as set out in UN R155.

What role do standards such as J1939 play here?
Interestingly, the scope and manner in which CV companies take advantage of standards and their capabilities are also quite heterogeneous. This ranges from extremely extensive use to implement own functions to rather more minimalist implementations strictly at interfaces that require support for the standard. Of course, a standard is particularly beneficial at junctures where the commercial vehicle ecosystem requires several manufacturers to cooperate, for example, for combining chassis and powertrain from different vendors – and even more so when add-on parts and bodies are sourced from different manufacturers.

Dr. Jan Holle is Product Field Manager Intrusion Detection & Prevention Solution (IDPS) at Escrypt, a brand of Etas in Stuttgart (Germany). Holle holds a diploma in computer science and a doctorate in electrical engineering. He has been working for Escrypt since 2013. He was initially working as a security engineer with a focus on IoT security and secure future EE architectures and before his current position as a product manager for in-vehicle network security solutions.

© Etas

In this case, companies can spare themselves a lot of coordination effort, enable flexible use, and even repurpose variants over the vehicle's life cycle. This approach could be also beneficial when developing future software-defined passenger cars. J1939 helps disentangle the development strands for different software components and component development as a whole, which also simplifies efforts to decouple development cycles and use of different development methods.

Do you see any drawbacks?
As with any development of a standard, the further development of J1939 requires a corresponding effort and the necessary time for industry-wide coordination. In this respect, adapting the standard to new technologies and market requirements quickly enough seems to me to be an ongoing challenge.

"The biggest difference is how to develop software together and specify the right software packages"

Is it a bigger advantage to have a shared ecosystem with more infrastructure or is the one-size-fits-all more of a disadvantage regarding differentiation?
These are valid concerns, of course, but standards and standard components also enable manufacturers to focus on their core competencies – that is, they can concentrate on the product or service attributes that are the decisive purchase factors for the customer. On top of that, we find that commercial vehicles have to suit very heterogenous customer purposes – and this they can only do with a combination of systems sourced from different manufacturers. If a vehicle manufacturer tried to offer everything from a single source, that company would have to support a vast quantity of variants – and possess the necessary domain knowledge. Economically speaking, that would hardly be feasible.

Can an intrusion detection system be a a silver bullet for security?
Absolutely not! An Intrusion Detection System (IDS) will always be a supplementary security solution. Let me stress that we have to first set up the fundamental security mechanisms in the vehicle. These are mechanisms such as secure firmware updates, secure on-board communication where it's needed, and of course secure diagnostic access. Each of these mechanisms has to come with strong cryptography, which could use hardware security modules with established automotive security software stacks. And secure software development is a must, always. Here too, we recommend reusing established security libraries. Only then can an IDS be sensibly implemented in the vehicle, which primarily has the task of detecting threats that are not yet known. In other words, suitable security measures need to be implemented to guard against all threats that are known at the time of the vehicle's development. Then an IDS can serve as a

© Etas

With some commercial vehicle manufacturers, you can see an agility that is more common in the car sector with startups and is possibly a result of the comparatively small company sizes and simpler organizational structures, says Holle

supplemental solution to protect against future – as yet unknown – threats.

How many commercial vehicle OEMs are already using or planning to use IDS?
IDS are most widespread in Europe, but commercial vehicle manufacturers in Asia – particularly in China – and in North America are following quickly. The main reason for the different take-up rates is that regulations vary from region to region. The biggest drivers in Europe are the UN R155 security requirements for type approval. China is currently developing comprehensive cybersecurity standards and regulations as well – the scope and depth of which go well beyond the requirements of UN R155.

Do the regulations you mentioned prescribe specific IDS technologies?
This is indeed the case in China, where requirements are formulated so clearly as to leave but a few degrees of engineering freedom. UN R155, by contrast, follows a risk-based approach with more degrees of freedom for the OEM. However, this regulation also gives very specific examples of typical threats and potentially suitable countermeasures, such as the detection of malicious messages on the CAN bus. I believe it will be hard to argue that these and similar requirements can be met efficiently and effectively without an in-vehicle monitoring solution such as IDS combined with fleet monitoring – that is, a Vehicle Security Operations Center or VSOC for short. Most OEMs – at least those in Europe – have therefore prepared or are preparing for the new regulations by integrating IDS components, setting up VSOCs, and taking other measures.

Does commercial vehicle systems' modularity have an impact on the approach to security as these systems are developed for many markets and suppliers?
Commercial vehicles do indeed present an additional challenge in terms of the IDS and other security measures: The security must be met as well as the modular CV ecosystem supported. Such security measures could entail cryptography to authenticate for diagnostic purposes or key management for secure on-board communication.

Do manufacturers cooperate on security issues?
They do, and we support this cooperation, for example, by taking part in and contributing to the relevant committees. For instance, there is a special interest group called the Commercial Vehicle Affinity Group, or CAG for short, for security issues in commercial vehicles within Auto-Isac. Of course, the committees of standardization organizations such as SAE and the like also communicate and cooperate on security topics.

What's your take on OTA updates in commercial vehicles – is this as easily manageable as in passenger cars?
I don't see any significant differences in terms of security, but of course we have to consider the issue of modularity. The question here is how to update individual components in the vehicle and any necessary add-on parts and body components via the air interface, while still achieving a consistent software status throughout the vehicle. However, this is not primarily a matter of security, at least not initially.

© Etas

Extensive standards and regulations for cybersecurity are currently being created in China, which in scope and depth even go well beyond the requirements of UN R155, explains Holle

© Etas

The increased use of non-differentiating, standardized software platforms could bring many advantages for manufacturers, and the reusability of software made possible by this makes economic sense, comments Holle

Let's talk about the smart truck/dumb trailer divide: Do you believe this will change at some point and what will it require?
I believe we're already seeing add-on parts that have an intelligence of their own. And in some cases, the necessary interfaces to the truck are already being implemented, for example, where physics prevent sensors from being installed in the truck. This trend is sure to pick up momentum in the future. From the security standpoint, we have to ensure that this kind of system does not cause additional vulnerabilities, and we have to attain at least the same level of security as for the actual truck. But we do have good cryptographic mechanisms and security concepts to securely implement these scenarios. This is why it is crucial for companies to arrive at an appropriate level of maturity in security engineering in their organizations, across the supply chain, and among partners in the ecosystem. Then these mechanisms and concepts can be put into action, properly and prudently.

"An intrusion detection system can serve as a supplemental solution to protect against future threats"

What is changing for vehicles because of electrification, for example due to additional communication options to charging stations?
Every additional interface and every added line of software code creates more complexity and thus engenders more security risks. Of course, this also applies to new interfaces such as those now serving to communicate with e-vehicle charging stations. These issues have already been addressed in the passenger car sector. Standards have been developed to describe certain specifications, for example, the cryptographic mechanisms needed to this end. They can also be used for commercial vehicles.

Could this type of intensive cooperation in certain areas be a model for the car market?
I would indeed like to see even more collaboration in the passenger car sector. The increased use of non-differentiating standardized software platforms would also benefit automakers in many ways. This allows software to be reused, which makes good business sense. It could also free up resources for developing core functionalities that set an automaker's vehicle apart. This trend is crucial to developing future vehicle functions, especially in the area of automated driving. We know that the software development capacities available today set absolute limits to the capacity to innovate. Better collaborative models and application of non-differentiating standardized software platforms will enable us to develop software-defined vehicles. These vehicles feature innovative software solutions based on the same non-differentiating software platform; solutions that manufacturers can use to persuade customers throughout vehicles' life cycles.

Mr. Holle, many thanks for the interview.

INTERVIEW: Robert Unseld