“Approach security with more pragmatism”

The automotive sector uses IT security specialists with many years of experience from other sectors. Sebastian Labitzke, responsible for security at ITK Engineering, explains in an interview how technology companies align these competences with automotive safety and security, and develop new processes and solutions.

Sebastian Labitzke has worked in the field of security at ITK Engineering AG since 2014. In addition to the disciplinary management of two security-engineering teams located in Rülzheim (HQ) and Berlin in Germany, he also coordinates ITK security projects on a company-wide basis. Due to his expertise in the area of IT security, he also oversees ITK’s information security management system. The focus of his expertise lies in the type identification of the attacker, the analysis of threat and risk, and the design of protocols to protect digital communication. Labitzke studied Information Technology at the University of Karlsruhe (TH) and obtained a doctorate from the Karlsruhe Institute of Technology (KIT) in Telematics with a security-related focus on identity and access management, and privacy enhancing technologies in the area of enterprise applications and online social networks. Working at the Steinbuch Centre for Computing (SCC) for six years gave him experience in projects for the SCC and for the network of computer centres belonging to the state universities of Baden-Württemberg, Germany.
ATZelektronik  Mr. Labitzke, ITK Engineering is a technology company, who mainly supports customers originating from the automotive industry to develop, integrate and safeguard control units and software. The subject of security is relatively new for ITK and the automotive sector – meaning that corresponding know-how must first be built up and acquired from other sectors. As a relative newcomer to security solutions, how do you convince your customers of your competencies?

LABITZKE  ITK has been investing in embedded security in the car for over six years. Automotive security itself is a new field of activity compared to classical IT-security that has had to deliver urgently required security solutions since the 90’s. Our security team, meanwhile with over 35 people, includes specialists with over ten years of experience in IT security and who have worked in other sectors with corresponding high-tech solutions: For all necessary disciplines such as IT security, protocol security (Telematics), mobile app security and embedded security.

In your opinion, what are ITK’s unique selling propositions compared to companies with long-serving IT security specialists?

We know the automotive business, the processes, the plans and the customer requirements very well. For over 22 years now, we have advised and developed solutions in the area of embedded systems, particularly in the field of safety and the implementation of security solutions. We have enriched our experience in the embedded domain with security know-how. We approach things very pragmatically. For example, we only advise in areas that we actually develop or implement ourselves. It may be that approaches, validated theories and well-meant guidelines for the implementation of security measures are available in written form. However the situation must be examined carefully so that each customer’s case and application can be interpreted individually to discover what is possible to achieve. Some companies start with a risk analysis and derive a plan of action from that and a few days later find themselves in a valley of despair faced with a the huge number of requirements and risks. The disappointment can be prevented, if those security-development engineers are tasked early enough with the analysis and implementation who come from the automotive embedded domain. These engineers know the restrictions in control units and are able to not only advise but also implement security. Only then do we have a realistic chance to arrive at a catalogue of security measures, a secure architecture and secure protocols that are actually implementable.

“The challenge is to find the balance between safety, security and costs. Which interdependencies, conflicting targets and synergies do you see? First of all, it is important to achieve a high level in terms of standards and integrated processes in security, as we have established with safety with the ISO 26262. This means that we must invest in this area. Cost is a decisive factor everywhere. These can be kept low by enabling the highest degree of synergy between safety and security as possible. It is not expedient to synchronise both disciplines in a mutual process, but rather by creating interfaces and enabling collaboration and cross-fertilisation.

Can you describe this with an example?

Some companies start with a risk analysis and derive a plan of action from that and a few days later find themselves in a valley of despair”, Sebastian Labitzke explains and refers to a more pragmatic approach.
safety engineer is to deploy the airbag in a dangerous situation at exactly the right moment and then as quickly as possible with the lowest possible latency time. The security engineer however, needs to guarantee that the deployment of the airbag is not erroneously triggered, for example by an external provocation. The vehicle developers achieve this by implementing cryptographic measures. These measures cost valuable time that the safety engineer has worked hard to eliminate. The conflict can only be solved with previously mentioned new processes …

… that have not been established yet and currently point to weaknesses? Currently it costs a lot of effort to achieve adequate and efficient processes. These need to be improved as soon as possible. In my view, many companies are well on the way to integrating security in early stages of the development process. Admittedly, it is an ambitious route that gives us as ITK the opportunity to achieve great things in consultation and accompaniment.

Is there a timetable for the pending improvements and further developments in the security sector? The development of standards is being discussed and successively worked out in committees. The basis for this task already exists. However a kind of security handbook will not be available in the near future and it would also not make any sense. Even if we were to work on standard architectures, at the end of the day, security must be developed individually, as modularly as possible and on the basis of state-of-the-art cryptography.

You previously emphasised collaborative and parallel development and now individual development.

It is not a contradiction. Cryptography itself has to develop further because the world of security is tremendously dynamic. The attackers of today are not able to do what they will no doubt master perfectly tomorrow. The defence strategy includes the modularity of security, for example the rapid exchange of processes for an intended update capability without recalling the entire vehicle fleet.

More and more experts are talking about a necessary revolution in the architecture of a vehicle and do not see much hope for evolutionary developments. What is your view? Both worlds will exist depending on how many features need to be developed on what timescale. Security experts are developing solutions for both approaches. Security can be integrated faster and better on revolutionary architectures, however in my view, it is not currently known whether this means it can be achieved faster in the system. It can be tested in a greenfield situation or in a periodically redesigned system. Evolutionary development will continue to prevail. It is revolutionary enough for the sector to migrate component-based architectures into function-oriented ones.

“New teams of security experts are required”

Consumer Electronics for the Automobile (CE4A) brings many challenges. Which special topics do you see? We need to master open systems and the multi-faceted challenges of connectivity means that automotive security engineers are faced with completely new tasks. For example, the consumer sector is introducing Apps that intervene with the vehicle control. This sets the alarm bells ringing and reaches the highest level of alert. New teams of security experts will be required from a variety of domains: IT security and automotive embedded. It also means that experts for protocols and architectures must sit at the same table as mobile app developers.

Does this table exist? At ITK, we have been bringing people from these domains together for six years. We live this exchange and it profits both security solutions and us enormously. At first, there were no such cus-
customer orders and we only executed the mutual engagement in work groups in internal projects. For example, we ran benchmarking for control unit cryptography algorithms for the security community. All this helps us with today’s series production – mainly regarding technical issues and executed maturity processes, but also with a view of building sustainable trusting relationships and a well-coordinated teamwork.

It took many years to build up and establish ISO 26262. The sector does not have the luxury of time for comparable security standards. How will you and your customers navigate this situation?
Indeed, we do not have time. And I make no excuses. However, I find the current processes of change and information-gathering full of tension, in a positive sense. In parallel to the current movement towards standardisation, the processes also need to be established. Those companies who occupy themselves with the on-going standardisation processes and are staying up-to-date by implementing continuous changes and adjustments to their organisations and products are creating a competitive advantage. And they are saving themselves the high costs of changes late in the game.

It is not only technical and procedural changes that are tremendously dynamic, but also the race for the best people, possible cooperations and acquisitions. In this context, how would you evaluate the start-up scene?

It is exciting to see how start-up companies act in the market, how attempts are made to integrate them and what relevance they receive in so doing. ITK is experiencing and leads this exchange very closely and we are working out perspectives. Start-ups and potential start-ups impart fantastic impulses that are unbelievably important for the automotive sector.

Mr. Labitzke, thank you for the informative discussion.