“Cyber security has arrived in all companies as a key challenge.” This is the summary of Dr. Thomas Beck, CEO of Vector, from his experiences with companies worldwide. In 2007 when the Vector Group presented in Baden-Baden and spoke for the first time regarding the growing relevance of security in the context of functional safety with a practical contribution and own solutions, many companies had argued that security is no issue in the automotive area. This attitude has changed completely, as the recent Vector Symposium 2016 showed. The widely attended Stuttgart Liederhalle assembled car manufacturers, suppliers and IT companies to share their experiences on cyber security. Excerpts of the event and many practical tips are provided in this article.

There is no absolute security

“There will be no absolute security, since each complex system bears defects.” This warning of Dr. Christof Ebert, Managing Director of Vector Consulting Services, gives a clear signal. Each company must establish a risk-oriented cyber security management that works reliably and traceable throughout the whole life cycle for its products, processes and supply chain. Experiences at Vector show that security is often limited to organically grown individual measures such as encryption. Crypto solutions, key management, code analysis, fuzz testing and firewalls are necessary, but their value is meager as long as vulnerabilities remain insufficiently addressed, be it consciously or unconsciously. About 90 percent of all security related incidents are due to human errors according to the experiences of Vector when surveying customers. The answer is a risk-oriented culture where security is specified across functions, systematically developed and continuously verified and validated. Figure 1 depicts this value chain, emphasizing in particular on dangers arising internally or externally. It would be naive to assume that attacks...
come only from the outside. Vulnerabilities are caused by careless development processes, unsystematic releases, but also by deliberate errors, such as “back doors” and “master access”. Companies have to secure the entire supply chain and in doing so deliberately change their perspective. It takes the ability to think like an attacker and on this basis take preventive actions as an engineer or manager. This protection must always work, especially when last-minute changes are implemented just before delivery, or variant regressions of a product appear years after the original release.

Holistic approach
Cyber security across industries has become a high commercial risk, since there is no absolute protection against hackers and abuse. Lorenz Slansky of Daimler AG underlines that cyber security is increasingly important for a brand, and consequently constitutes a competitive advantage. For critical systems, such as in-vehicle information, security is highly relevant and cannot be compromised by insufficient usability. Key issues in the development of protective systems are the complete identification of security requirements, the systematic implementation of security functions and security checks with the goal of consistent evidence that all the relevant security requirements are met. Security standards such as SAE 3061 help to learn from other industries and thus quickly implement essential solutions. Lorenz Slansky knows that proprietary mechanisms often pretend just supposed security and clarifies: “Security by obscurity does not prevent hackers, but delays good solutions” Dr. Christian Meineck of Porsche AG adds: “Security concepts must consider the vehicle and the IT networks inside and outside the vehicle.” Figure 2 shows a subset of typical attack scenarios, and how they are evaluated by manufacturers. The times of individual functional units are gone, and the complex vehicle system demands solutions as they are already practiced today in complex IT systems, such as continuous software upgrades in a very short time and of course “over the air” (OTA). Standards foster fast learning from the IT by cross-fertilization and thus prevent that errors are repeated in every industry again and again.

Due to the high degree of interconnected functions in the vehicle but also to the outside by increasingly open interfaces not only a specific function is affected, but also other functions that belong to a system group and interact with this specific function. This includes non-electrical characteristics. For example, a warning of mechanical problems or wear-out may no longer function after a functional incident or attack on a bus system. Masahiro Goto and Martin Prisching of DENSO showed that safety and security aspects must be considered as a pair. To achieve this, the attack tree analysis (ATA) is supplemented by the Fault Tree Analysis (FTA) in order to systematically cover both type of risks. It is obvious for them that “all layers of the security architecture must be addressed for continuous security to achieve the well-known concept of ‘Defense in Depth’. Figure 3 shows with the example of Cooperative Adaptive Cruise Control (CACC) how various security measures protect against threats in the network.

Katharina Lohmann of Hella observes specifically in verification and validation a huge need to move forward. While process frameworks such as SPICE are used to systematically prevent errors in engineering and maintenance, there is an urgent need to improve verification such as systematically scanning each new software regression before further testing and delivery, as well as introducing new testing procedures as fuzz testing and penetration testing.

![Figure 1: Risk-oriented Security must consider the entire life cycle.](image-url)
Dr. Günther Heling of Vector highlights from his own experience in development and delivery of advanced AUTOSAR basic software that only an automatic supply chain with rigorous release criteria creates the necessary quality.

Cryptography as a solution
Cryptographic methods are today an essential part of security solutions. Klaus Schmeh of cryptovision assumes that the AES encryption procedure with 10 to the power of 38 possible keys will not be cracked in the foreseeable future even with quantum computers. A major challenge is to integrate this and other security mechanisms in a meaningful way to vehicle IT systems. High performance requirements often contradict and eventually inhibit security, as

Dr. Andre Weimerskirch of the University of Michigan emphasizes. In the world’s largest field test of Public Key Infrastructure (PKI) for car-to-car (C2C) and car-to-infrastructure (C2I) communication, he combined performance requirements and data protection. His logic is simple: “Priority one is functional safety, and priority two is privacy.” Dietmar Hilke of Thales develops solutions for advanced security requirements. Design for security to his experience is an important tool, and he cross-fertilizes medical immunology with IT. Just as there are multi-resistant germs, the attacks are constantly developing new patterns. With systemic resilience the resistance will be expanded continuously. Security begins in design, but is a task for the entire lifecycle – no matter how long that is.
The companies agree that consistent risk-oriented security cannot solely be achieved by patches on ECU and network level. Security needs to address the overall architecture. Figure 4 shows the reference model of Vector with a clear separation of subnets. Between these subnets firewalls and intrusion detection systems are placed. Dr. Eduard Metzker of Vector sees such distributed security architectures under the current environmental circumstances as the best way, because they can be implemented in a step-wise mode. This requires a layered security architecture as it is propagated by Denso and other Tier-1 suppliers. Starting with a hardware-based anchor and AUTOSAR with its state-of-the-art crypto solutions, the individual components are individually hardened. Dr. Achim Fahrner of ZF emphasizes in this layering the importance of a crypto-co-processor and hardware security module (HSM) to build resilience and robustness bottom-up. The communication to safety-critical subsystems like steering and brakes should have no direct connection to infotainment and other vulnerable systems. This is especially true in ‘Over the Air’ (OTA) upgrades that are increasingly being used. Axel Freiwald of Infineon underlines that while OTA reduces the number of callbacks, it must also be carefully protected before it is used in existing networks. Not only are the IT requirements growing, such as rollback and availability, but also the secure distribution of software to the respective control units. Companies must strengthen their competences in cyber security solutions, as well as systems and IT architecture in order to progressively modularize the organically grown architecture. At the same time they need to implement a strategy for sustainable support of various organizational units. Operationally this can be steered by a security manager, who is responsible for the release of architectures and component releases. The traditional change control boards need to be strengthened technically but also in the way they are working, to evaluate the threats on the basis of defined criteria and assess different solutions before implementation. Periodic architecture reviews and adjusting the test strategy with focus on security will deepen the mutual understanding among developers and managers that security measures are not a straw fire, but must be implemented in each single project. Such concepts cannot simply be imposed: They need strong anchor points in the organization. Vector reports from its projects that such behavioral changes make security sustainable because the teams have a tangible and concrete responsibility.

Security needs systematic handling
The cyber security projects of Vector give one clear message: The line between systematic implementation of automotive cyber security and ineffective ad-hoc measures is small and thus requires professional assistance. Security attacks exhibit a common pattern where strength does not exploit weakness but intelligence does exploit recklessness. This means for instance errors in the configuration of firewalls and gateways, not fully coherent software changes, and complicated user interfaces so that security measures remain in their default status and are thus vulnerable to attacks. On the basis of threat assessments, provisioning dedicated infrastructure components and tools for verification and monitoring, up to architecture reviews and

Figure 4: Security by design in practice: Different subnets should be separated as much as possible
security consulting Vector has gained wide experiences. Only a consistent life-cycle will facilitate cyber security: From the initial hazard analysis to architectural decisions, verification to regression tests at each new delivery and after-sales change management. That is also the impulse of Prof. Ebert of Vector: "Sustainable cyber security, that ought to be more than a flash in the pan, needs continuity and cooperation with professionals."

For more information on Cyber Security and Access to the mentioned presentations and videos, please visit: www.vector.com/security

Translation of a German publication in Elektronik automotive, special issue on Software September 2016

Image rights:
Teaser image: Vector Informatik GmbH
Image 1: Vector Consulting Services GmbH
Image 2: Porsche AG
Image 3: Denso Automotive GmbH
Image 14 Vector Informatik GmbH