Making security in automotive IT systems holistic, economically efficient, and structured

As automotive IT systems become ever more closely networked, they must be protected against unauthorized manipulation to ensure the safety of all road users. This calls for holistic and structured approaches to security that utilize available resources as economically as possible. One such holistic security concept that holds great promise – both within companies and between sectors – introduces safety classifications consisting of security levels and security profiles.

Looking at the Big Picture

AUTHORS

Dr. Martin Emele is Head of the Security Product Group at **ETAS GmbH**.

Dr. Benjamin Glas is an expert on cryptography and secure communication at **ETAS GmbH**.

Dr. Marko Wolf is Head of Engineering at **ESCRYPT GmbH**.

Dr. Thomas Wollinger is Managing Director of **ESCRYPT GmbH**.

Whether in the automotive or home appliance sectors, or in the growing internet of things, enormous challenges lie ahead for embedded security. Modules that used to be self-contained are now opening up within overall systems – and also outwardly to the internet. This is driving up the numbers of attack vectors, weak points, and simple sources of error. Ensuring a product functions dependably is no longer simply a question of functional safety but also one of IT security. While safety is all about making sure products function correctly, security is concerned with protecting the integrity, intellectual property, and – more and more – also users' personal data.

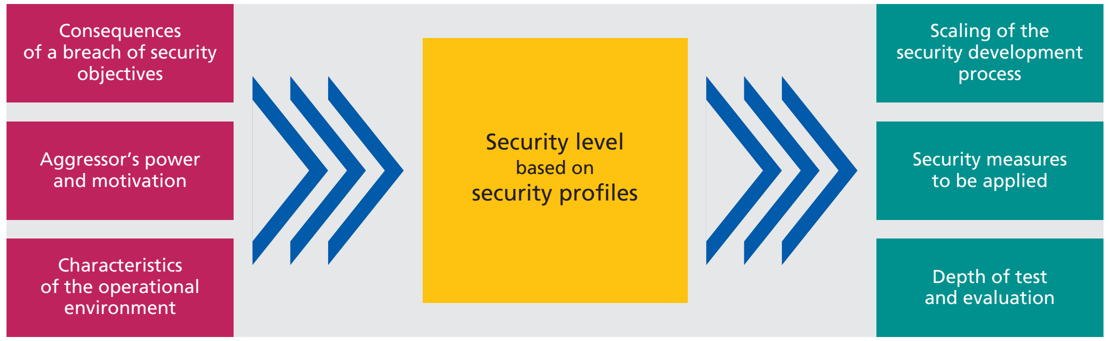
The weakest link breaks first

Regardless of whether a breach was caused by a malicious aggressor or by technical failure, it is the weakest part in the overall system that is responsible for its security. In the automotive sector it is particularly important to keep this precept in mind when considering its widely distributed development processes and value creation chains. Standardized safety classifications offer a structured, holistic framework which ensures that development resources for security are utilized at an early stage and in a way that is both functional and economically focused. Classifications help to answer two fundamental questions: "What exactly must be protected?" and "How good must the protection be?" The aim of security is to protect value. But for each value, different aspects need protection. The most important aspects are confidentiality, integrity, and authenticity, along with availability. Each system or subsystem gives the protection of these aspects a different weighting. This feeds into a security profile that at the domain level is often characteristic for a class of systems. A security profile answers the question "What exactly must be protected?" in the form of a vector with scale values for the various security aspects.

How good must each thing's protection be?

The necessary level of protection can be determined by assessing the risk of threats. The expected consequences or costs that might result from a breach of the security objectives are to be considered. They are more significant, for instance, if a brake fails than if an engine sensor stops working. Another consideration is the likeliness of a security breach occuring. Factors such as capability, resources, prior knowledge, time frames for an attack, and the aggressor's motivation must be taken into account in this context. Taken together, the "What?" and the "How good?" set out the security level, which quantifies various degrees of required protection strength, ranging from none to very high.

The security profile, however, makes it possible to purposefully select security measures from a continuously updated range of recommended protective measures. For each domain, it is possible to define packages of measures that reflect the different profile requirements and constitute a framework for the security concept. This guarantees that proven, standardized methods can be employed in a coordinated way and correctly configured, while ensuring there is a continuous improvement process in place that also extends beyond system and company limits.


Consequences of a breach of security objectives
Aggressor's power and motivation
Characteristics of the operational environment
Security level based on security profiles
Scaling of the security development process
Security measures to be applied
Depth of test and evaluation

By means of a risk analysis, products and systems are assigned a security profile and a security level. The security measures and development process are derived based on this classification.

Approaches from other domains

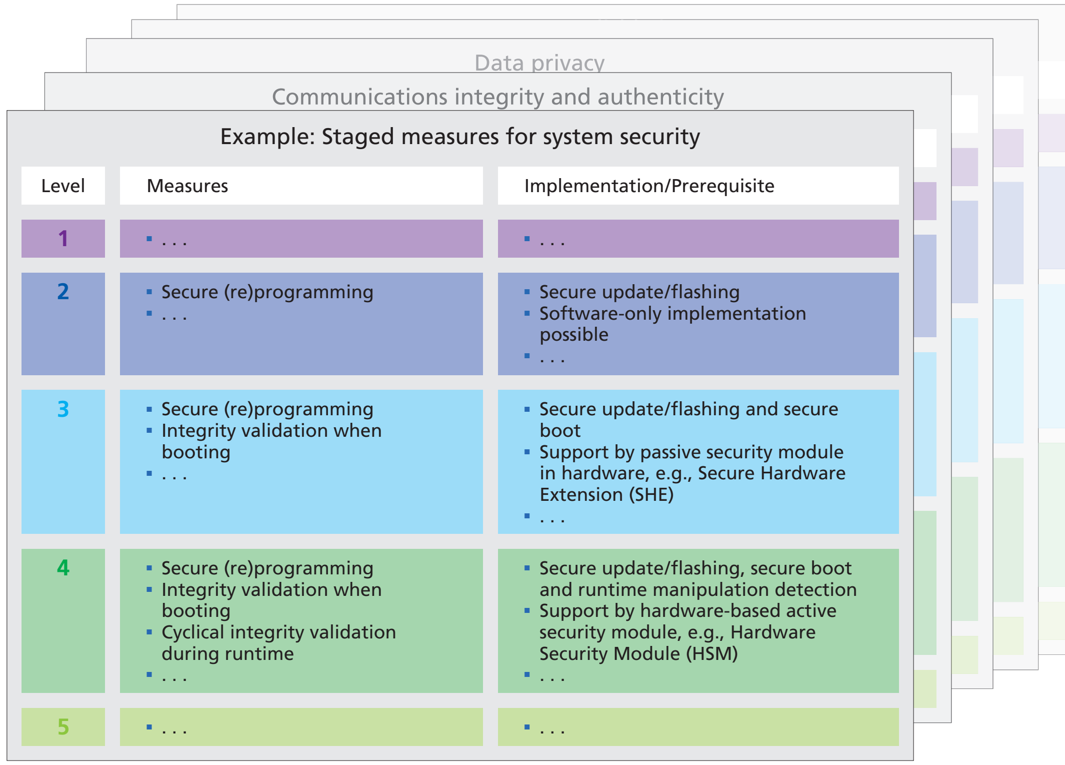
Numerous approaches have already been used and validated in other domains that can provide a useful basis for further action. The evaluation and assurance subarea, for instance, can turn to the Common Criteria (CC) as a detailed and internationally recognized framework. The IT baseline protection outlined by BSI, Germany's Federal Agency for Security in Information Technology, consists of simple rules for identifying and implementing security measures in IT systems using the very latest technology. Meanwhile, in the area of automation technology, the IEC 62443 standard concerns itself with security levels for products and IT systems.

Last but not least, for the automotive sector, ISO 26262 provides a comprehensive, tailored set of rules with various safety levels (ASIL – Automotive Safety Integrity Level) and process specifications. However, no procedure has yet emerged that is directly tailored to the automotive security field and applicable throughout the entire life cycle.

Industry-wide adoption offers the greatest benefit

Once they have been introduced within a company, safety classifications for security cut development costs and keep security levels consistent across all product classes. But to get the most out of this type of concept, it needs to be adopted industry-wide and based on harmonized standards. Organizations such as ISO, AUTOSAR, or SAE are internationally established bodies for implementing a structured security concept. ETAS and ESCRYPT can assist manufacturers and vendors in all areas – from analysis of threats and risks through the definition of security levels and on to the selection of suitable test and analysis methods – not only in development but also in operational series production. This enables them to meet the respective protection objectives securely and with an economically efficient use of resources.

Example of staged measures for different security levels


Data privacy
Communications integrity and authenticity

Example: Staged measures for system security

Level	Measures	Implementation/Prerequisite
1	▪ . . .	▪ . . .
2	▪ Secure (re)programming ▪ . . .	▪ Secure update/flashing ▪ Software-only implementation possible ▪ . . .
3	▪ Secure (re)programming ▪ Integrity validation when booting ▪ . . .	▪ Secure update/flashing and secure boot ▪ Support by passive security module in hardware, e.g., Secure Hardware Extension (SHE) ▪ . . .
4	▪ Secure (re)programming ▪ Integrity validation when booting ▪ Cyclical integrity validation during runtime ▪ . . .	▪ Secure update/flashing, secure boot and runtime manipulation detection ▪ Support by hardware-based active security module, e.g., Hardware Security Module (HSM) ▪ . . .
5	▪ . . .	▪ . . .