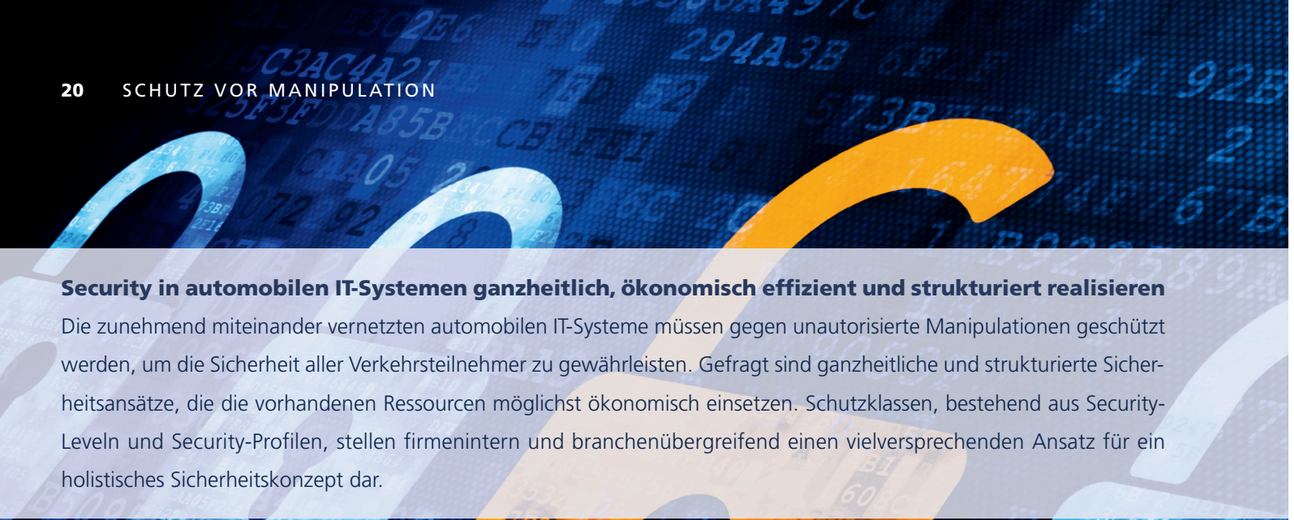


Security in automobilen IT-Systemen ganzheitlich, ökonomisch effizient und strukturiert realisieren

Die zunehmend miteinander vernetzten automobilen IT-Systeme müssen gegen unautorisierte Manipulationen geschützt werden, um die Sicherheit aller Verkehrsteilnehmer zu gewährleisten. Gefragt sind ganzheitliche und strukturierte Sicherheitsansätze, die die vorhandenen Ressourcen möglichst ökonomisch einsetzen. Schutzklassen, bestehend aus Security-Leveln und Security-Profilen, stellen firmenintern und branchenübergreifend einen vielversprechenden Ansatz für ein holistisches Sicherheitskonzept dar.

Aufs Ganze gesehen

AUTOREN

Dr. Martin Emele ist Leiter des Produktbereichs Security bei der **ETAS GmbH**.

Dr. Benjamin Glas ist Experte für Kryptographie und sichere Kommunikation bei der **ETAS GmbH**.

Dr. Marko Wolf ist Head of Engineering bei der **ESCRYPT GmbH**.

Dr. Thomas Wollinger ist Geschäftsführer der **ESCRYPT GmbH**.

Ob im Automobilbereich, bei Haushaltsgeräten oder im wachsenden Internet der Dinge – auf die Embedded Security warten enorme Aufgaben. Früher geschlossene Baugruppen öffnen sich innerhalb des Gesamtsystems und auch nach außen zum Internet. Dadurch vervielfältigen sich Angriffsvektoren, Schwachstellen und simple Fehlerquellen. Die sichere Funktion eines Produkts hängt nicht mehr nur von der Funktionalen Sicherheit (Safety), sondern auch von der (IT) Security ab. Safety kümmert sich um die korrekte Funktion, Security schützt die Integrität, das geistige Eigentum und immer öfter auch die persönlichen Daten des Anwenders.

Das schwächste Glied bricht zuerst

Ganz gleich, ob es um mutwillige Angreifer oder um technisches Versagen geht, entscheidend für die Sicherheit ist die schwächste Stelle im Gesamtsystem. Gerade im Automobilbereich ist es wichtig, diese auch bei den weit verteilten Entwicklungsprozessen und Wertschöpfungsketten im Blick zu behalten. Standardisierte Schutzklassen bieten einen strukturierten und holistischen Ansatz, um Entwicklungsressourcen für die Security frühzeitig und funktionell sowie ökonomisch zielgerichtet einzusetzen. Sie helfen, zwei Kernfragen zu beantworten: „Was genau muss geschützt werden?“ und „Wie gut muss der Schutz sein?“

Security zielt auf den Schutz eines Wertes ab. Aber bei jedem Wert sind andere Aspekte schützenswert. Die wichtigsten sind Vertraulichkeit, Integrität und Authentizität sowie die Verfügbarkeit. Jedes System oder Teilsystem gewichtet den Schutz dieser Aspekte anders. Daraus entsteht ein Security-Profil, das oftmals domänenspezifisch charakteristisch für eine Klasse von Systemen ist. Ein Security-Profil beantwortet die Frage nach dem „Was ist zu schützen?“ in Form eines Vektors mit Skalenwerten für die verschiedenen Security-Aspekte.

Was ist wie gut zu schützen?

Wie gut der Schutz sein muss, lässt sich durch eine Abschätzung des Bedrohungsrisikos feststellen. Zum einen spielen die zu erwartenden Konsequenzen oder Kosten eine Rolle, die durch eine Verletzung der Sicherheitsziele entstehen könnten. Sie liegen beispielsweise beim Versagen einer Bremse höher als beim Ausfall eines Motorsensors. Zum anderen muss die Eintrittswahrscheinlichkeit einer Sicherheitsverletzung betrachtet werden. Hier sind Faktoren wie Fähigkeiten, Ressourcen, Vorkenntnisse, Zeitfenster für einen Angriff und Motivation des Angreifers zu berücksichtigen. Das „Was?“ und das „Wie gut?“ ergeben zusammen den Security-Level. Er quantifiziert die Stärke des Schutzes in verschiedenen Abstufungen von kein bis sehr hoher Schutzbedarf.

Das Security-Profil hingegen ermöglicht die zielgerichtete Auswahl von Security-Maßnahmen aus einem kontinuierlich aktualisierten Katalog empfohlener Schutzmaßnahmen. Domänenspezifisch können Maßnahmenpakete definiert werden, welche die unterschiedlichen Profilanforderungen abbilden und einen Rahmen für das Security-Konzept bilden. So wird sichergestellt, dass erprobte, standardisierte Verfahren aufeinander abgestimmt eingesetzt und korrekt konfiguriert werden und ein kontinuierlicher Verbesserungsprozess auch über System- und Unternehmensgrenzen hinweg besteht.

Mittels einer Risikoanalyse werden Produkte und Systeme einem Security-Profil und einem Security-Level zugeordnet. Anhand dieser Klassifizierung leiten sich die Security-Maßnahmen und der Entwicklungsprozess ab.

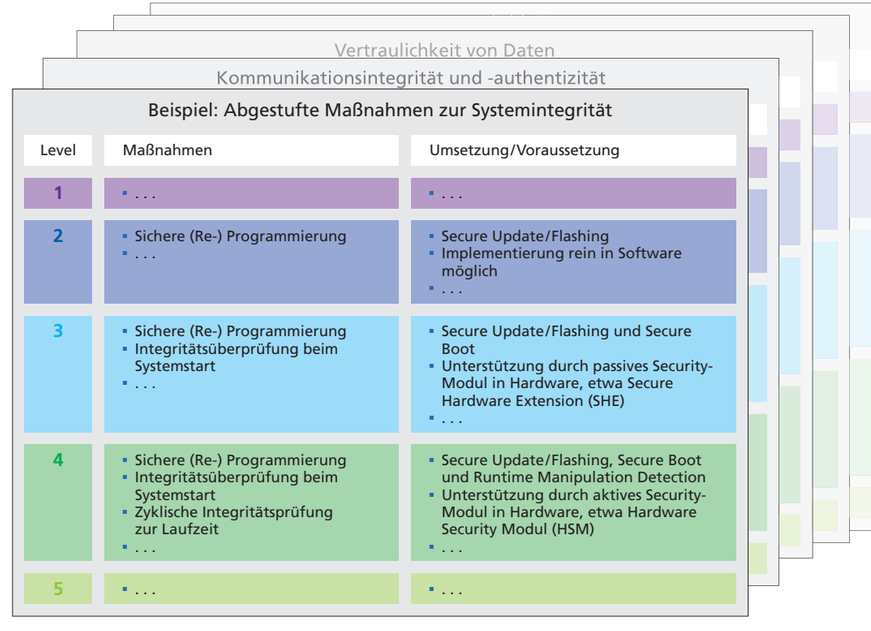
Ansätze aus anderen Domänen

In anderen Domänen gibt es bereits zahlreiche Ansätze und ähnliche Erfahrungen, die eine gute Grundlage für das weitere Vorgehen liefern. Für den Teilbereich Evaluierung und Assurance bieten etwa die Common Criteria (CC) einen detaillierten und international anerkannten Rahmen. Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) enthält einfache Regeln, um in IT-Systemen Sicherheitsmaßnahmen nach dem aktuellsten Stand der Technik zu identifizieren und umzusetzen. Und im Bereich der Automatisierungstechnik beschäftigt sich der IEC 62443-Standard mit Security-Leveln für Produkte und IT-Systeme.

Nicht zuletzt existiert mit der ISO 26262 ein für den Automobilbereich zugeschnittenes, umfangreiches Regelwerk mit verschiedenen Safety-Leveln (ASIL – Automotive Safety Integrity Level) und Prozessvorgaben. Allerdings existiert bisher kein Verfahren, das direkt auf den Automotive Security-Bereich angepasst und über den ganzen Lebenszyklus anwendbar ist.

Größter Nutzen bei branchenweiter Einführung

Firmenintern eingeführt, sparen Schutzklassen für Security Entwicklungskosten und halten den Security-Level über Produktklassen hinweg konsistent. Den größten Nutzen bringt ein solches Konzept jedoch, wenn es branchenweit angenommen und über Standards harmonisiert wird. Gremien wie ISO, AUTOSAR oder SAE sind international etabliert, um ein abstrahiertes Security-Konzept einzuführen. ETAS und ESCRYPT können Hersteller und Zulieferer dabei in allen Bereichen, von der Bedrohungs- und Risikoanalyse über die Definition der Security-Level bis hin zur Auswahl geeigneter Test- und Analysemethoden, unterstützen – und das nicht nur bei der Entwicklung, sondern auch im operativen Serienbetrieb. So können die jeweiligen Schutzziele sicher und mit ökonomischem Mitteleinsatz eingehalten werden.



Beispiel für abgestufte Maßnahmen für verschiedene Security-Level