Hacker-in-the-Loop

© Getty Images/Cecilie_Arcurs

Moderne softwaregesteuerte Fahrzeugsysteme müssen nicht mehr nur funktional sicher sein, sie brauchen auch Schutz gegen Angriffe von Cyber-Kriminellen. Um den Schutz der Steuergeräte gegen Cyber-Attacken im Kontext des Gesamtfahrzeugs zu testen, setzen ETAS und ESCRYPT auf umfassende Angriffssimulationen im HiL-/SiL-Testumfeld und Virtualisierung. Die Vorteile der HiL-/SiL-(XiL)Technologie werden so auch für Security-Tests nutzbar.

Ein Alptraum: Hacker verschaffen sich Zugriff auf ein Fahrzeugsystem, fangen Sensorsignale ab und speisen stattdessen korrumpierte Daten in das Onboard-Netzwerk ein. Aus heiterem Himmel wäre der Fahrer machtlos und säße in einem fremdgesteuerten Fahrzeug. Um solche Szenarien zu verhindern, sind im vernetzten Automobil verlässliche Security-Lösungen gefragt.

Doch wie lassen sich diese Security-Lösungen wirkungsvoll auf mögliche Hackerangriffe testen? Wie kann man sicherstellen, dass sie mögliche Cyber-Attacken richtig erkennen und effektiv abwehren? Und wie kann man Security schon am Anfang des Entwicklungsprozesses effizient prüfen, um mögliche Schwachstellen nicht erst kurz vor der Auslieferung festzustellen, wenn die dann notwendigen Schutzmaßnahmen kaum noch sinnvoll zu realisieren sind?

Zum Glück kann Cyber-Security auf bereits etablierte Maßnahmen aus dem Bereich der funktionalen Sicherheit (Safety) aufsetzen. Dort sind zum Beispiel Steuergeräte-Testansätze wie Hardware-in-the-Loop (HiL) und Software-in-the-Loop (SiL) etabliert, um bereits während des Entwick-

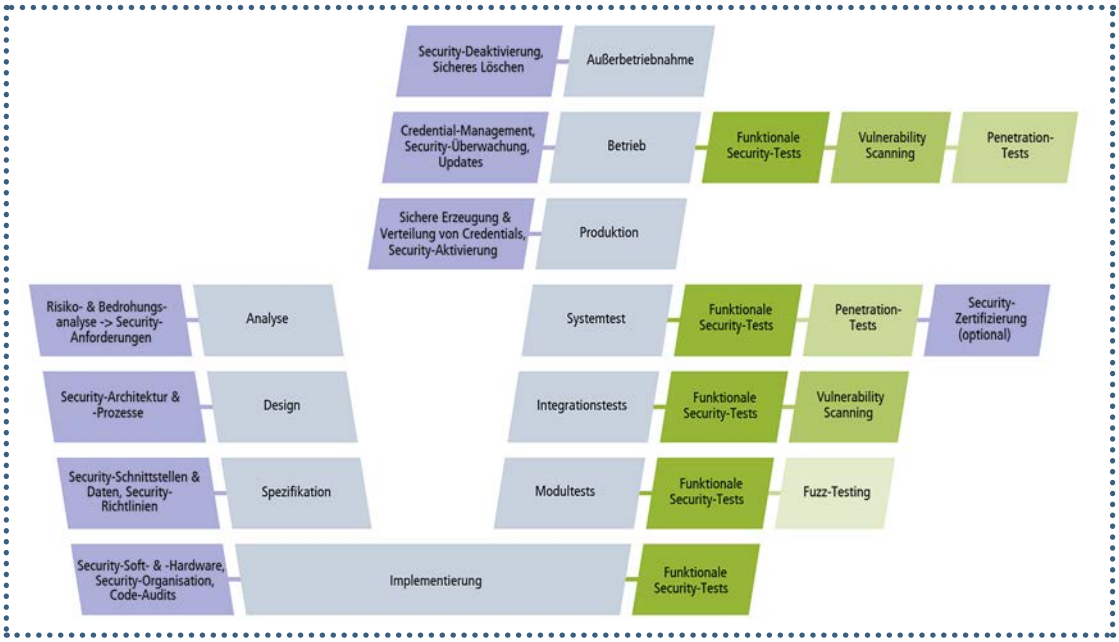

Bild 1: Security-Tests (grün) und weitere Security-Aktivitäten (violett) im automobilen Entwicklungszyklus. Erst der umfassende Ansatz mit entsprechenden Tests bringt wirklich Sicherheit. (© ESCRYPT)

lungsprozesses zu prüfen, dass Steuergerätefunktionen im Normalbetrieb und bei Störungen wie vorgesehen reagieren. Dabei testen Entwickler die Steuergeräte nicht nur einzeln, sondern auch in Interaktion mit Sensoren und anderen Steuergeräten als Teil einer Fahrzeugdomäne oder im gesamten Fahrzeug, inklusive aller Netzwerkteilnehmer und Datennetze. Echtzeit-HiL-Systeme wie ETAS LABCAR oder mit ETAS ISOLAR-EVE erzeugte virtuelle Steuergeräte bieten die dafür notwendige technologische Basis.

Neue Herausforderung: Hacker-in-the-Loop

Die Herausforderung für die zusätzlichen Security-Tests sind weniger die Testwerkzeuge, sondern vor allem die neue, andere Vorgehensweise bzw. die erweiterte Testmethodik. Für Security-Tests reicht zum Beispiel die „True-Positive-Methode", also das Abprüfen eines erwarteten Verhaltens, allein nicht aus, da viele Angriffsszenarien zum Zeitpunkt der Entwicklung noch unbekannt sind. Stattdessen gilt es, systematisch sowohl bekannte Schwachstellen als auch eventuelle neue, noch unbekannte Einfallstore bestmöglich auf potenzielle Security-Risiken abzuprüfen, oft oder gerade vornehmlich abseits der bekannten Spezifikationen und üblichen Prozeduren. Auch dafür eignen sich SiL- oder HiL-Testumgebungen hervorragend.

ETAS und ESCRYPT haben diese neue Herausforderung früh erkannt und ihr Know-how aus den Bereichen Automotive Safety- und Security-Testen optimal zusammengeführt. Ausgangspunkt für den erweiterten Testansatz ist das bekannte LABCAR-Testsystem mit dem Linux-basierten Simulationstarget LABCAR-RTPC (Real-Time-PC). Es ermöglicht »

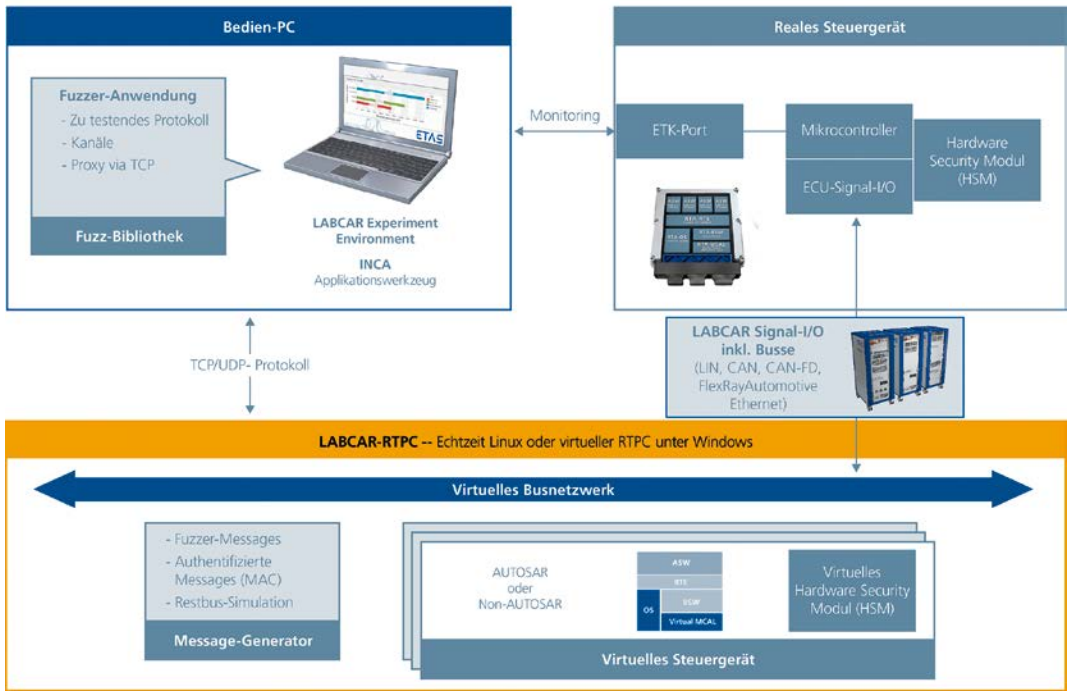

Bild 2: Prinzipieller Aufbau eines Security-Testsystems für Fuzzing-Tests. Mit dem ETK-Port hat der Tester Zugang zum Mikrocontroller. Die virtuellen Steuergeräte laufen auf dem LABCAR-RTPC. (© ETAS)

Safety- und Security-Tests mit realen (HiL) und auch virtuellen Steuergeräten (SiL), z. B. auf Basis von ISOLAR-EVE. Diese Tests in realistischen Fahrzeugumgebungen, inkl. verschiedener Fahrszenarien, kombinieren die umfangreiche Tool-Erfahrung von ETAS mit der langjährigen Automotive-Security-Expertise von ESCRYPT Dabei kommt ein automatisiertes Test-Framework zum Einsatz, welches zusätzlich zu den bekannten Safety-Testfällen nun auch Security-Testfälle generieren und auswerten kann.

LABCAR für Security-Tests

Solche Security-Tests umfassen zum Beispiel:

- Funktionale Security-Tests bezüglich Korrektheit, Zeit- und Ressourcenverbrauch neuer softwarebasierter Automotive-Security-Funktionen (z. B. AUTOSAR SecOC), neuer hardwarebasierter Security-Funktionen (z. B. Hardware-Security-Module wie SHE oder HSM) oder deren Kombination (z. B. Secure Boot).
- Vulnerability-Scans, das heißt die Überprüfung auf bereits bekannte Security-Schwachstellen auf Basis einer stetig aktualisierten dezidierten Automotive-Security-Angriffsdatenbank, wie UDS-Security-Exploit oder CAN-Spoofing.
- Fuzzing-Tests zur Entdeckung möglicher, noch unbekannter Security-Schwachstellen auf Basis systematisch erzeugter „Zufalls-Eingaben", die z. B. inhaltlich oder chronologisch von der Spezifikation abweichen, um möglicherweise verwundbares Fehlverhalten, wie Abstürze oder Funktionssprünge, gezielt zu provozieren.

Anhand der jeweiligen Reaktionen einzelner und mehrerer Steuergeräte im Verbund lassen sich mit diesen Security-Tests bekannte und teilweise noch unbekannte Schwachstellen in der Fahrzeug-IT frühzeitig aufdecken und beheben. Glücklicherweise ist nicht jede neu entdeckte Abweichung vom vorgesehenen Verhalten gleich ein Safety- oder gar ein Security-Problem oder jede mögliche Schwachstelle gleich ein reales Sicherheitsrisiko. Daher belassen es ETAS und ESCRYPT nicht nur bei der Bereitstellung der notwendigen Simulations- und Testwerkzeuge, sondern bieten zudem auch kompetente Beratung unter anderem zu:

- Aufbau/Konfigurieren der Testumgebung
- Erstellen individueller Testpläne und Testfälle
- Auswertung und Bewertung der Testergebnisse
- Erstellung möglicher Schutzmaßnahmen, insbesondere für den Bereich Cyber Security

Die Tester haben mit dem ETK-Port vollen, zeitsynchronen Zugriff auf Speicher und die interne Datenverarbeitung der Steuergeräte und können Prozesse exakt nachvollziehen. Erst diese Echtzeitmechanismen ermöglichen Analysen in der nötigen Breite und Tiefe.

Fazit

ETAS und ESCRYPT haben über viele Jahre hinweg gemeinsam umfangreiche Kompetenzen im Bereich HiL-/SiL-Technologien und Automotive Security aufgebaut. Diese gebündelte Kompetenz hilft nun Herstellern und Entwicklern, vernetzte Fahrzeuge bezüglich Safety und Security rundum zuverlässig abzusichern. Dabei bieten die etablierten HiL-/SiL-Testsysteme die optimale Ausgangsbasis, um beide Sicherheitsdimensionen möglichst früh, effizient, vollständig und wirksam zu prüfen, um damit den neuen Anforderungen an die Zuverlässigkeit des vernetzen Automobils gerecht zu werden. ■ (oe)

» **www.etas.com**
» **www.escrypt.com**

» **www.hanser-automotive.de/5222656**

Hier finden Sie die Download-Version des Beitrags.

Dr.-Ing. Tobias Kreuzinger ist Senior Manager Test and Validation bei ETAS in Ann Arbor, Michigan, USA.

Dr.-Ing. Marko Wolf ist Head of Consulting & Engineering von ESCRYPT.

Jürgen Crepin ist Fachreferent Marketing für die Bereiche Software Engineering und Security bei ETAS in Stuttgart.