DRIVING **EMBEDDED EXCELLENCE**

ETAS

RealTimes

2017/2018

www.etas.com

Christopher White
Executive Vice President Sales

Friedhelm Pickhard
President

Bernd Hergert
Executive Vice President Operations

Liebe Leserinnen, liebe Leser,

wir stehen mitten in einer sehr spannenden Phase der Entwicklung von Automobilelektronik. Der Trend geht immer mehr in Richtung intelligente, über die Cloud vernetzte und (teil-)automatisierte Mobilität. Dabei spielen die Themen Effizienz, alternative Antriebssysteme, vernetzte Bewegung und Verbindung zum Internet der Dinge eine zentrale Rolle. Doch ohne überzeugende Security und ohne umfassende Sicherheitskonzepte wird es kein autonomes Fahren geben.

In Zeiten der fortlaufenden Digitalisierung gilt es, besonderes Augenmerk auf die Systemsicherheit zu legen. Vernetzte Fahrzeugsysteme brauchen zusehends Schutz gegen unautorisierte Zugriffe auf Daten und Funktionen. Cyber-Security ist inzwischen ein essentieller Baustein, der über den gesamten Lebenszyklus kontinuierlich überprüft und angepasst werden muss. Vernetzte Fahrzeuge benötigen lernende Abwehrsysteme, die direkt auf neue Angriffsszenarien reagieren können. Im Automobilbereich sind wir bereits heute mit unserer Tochtergesellschaft ESCRYPT ein starker Anbieter von kompetenten Security-Lösungen – unser Ziel ist es, zukünftig ganzheitliche Cyber-Security-Lösungen für den wachsenden Security-Bedarf im Umfeld des IoT aufzubauen.

Mit dieser Ausgabe der RealTimes möchten wir Ihnen zeigen, wie sich ETAS und ESCRYPT als technik- und elektronikbegeisterte Unternehmen aktuellen Herausforderungen stellen und sie erfolgreich meistern. Beiträge zu neuen ETAS-Lösungen, wie zum Beispiel INCA-RDE, unsere Softwarelösung, mit der Real Driving Emissions-Testfahrten kontrolliert und reproduzierbar durchführbar sind, oder unsere neue SCODE-Produktfamilie zur modellbasierten Funktionsentwicklung, beschreiben die vielseitigen Anwendungsmöglichkeiten unseres Portfolios. Die Erfolgsgeschichten unserer Kunden zeigen die Vorteile in der Praxis. Unsere enge Zusammenarbeit mit Forschungseinrichtungen stellen wir Ihnen ebenfalls vor – ein zentraler Baustein, um unser Know-how auf hohem Niveau zu halten und unsere Lösungen permanent den Anforderungen neuer Technik anzupassen beziehungsweise zu optimieren.

Liebe Leserinnen und Leser, wir wünschen Ihnen spannende Einblicke und freuen uns, gemeinsam mit Ihnen zukunftsorientierte Lösungen zu entwickeln. Herzlichen Dank für Ihr Vertrauen und das Interesse an unserer Arbeit. Wir freuen uns auf eine gemeinsame Zukunft!

Friedhelm Pickhard Bernd Hergert Christopher White

Inhalt

Ethernet-Security

AUTOREN

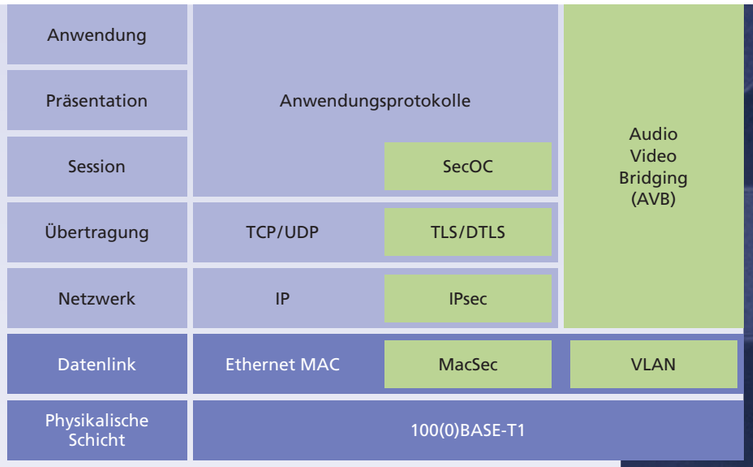
Norbert Fabritius und **Ramona Jung** sind Security Engineers bei der **ESCRYPT GmbH**.

Dr. Jan Holle ist Security Engineer und Produktmanager bei der **ESCRYPT GmbH**.

ESCRYPT ist eine hundertprozentige Tochtergesellschaft von ETAS und bietet Sicherheitslösungen im Bereich Embedded Security an.

Sicheres Ethernet – eine Chance für die Fahrzeug-IT

Seit über 40 Jahren ist der Ethernet-Standard in der klassischen IT etabliert. In Rechenzentren und im Consumer-Bereich ist er eine feste Größe. Nun erobert er moderne Fahrzeuge. Nach ersten Einsätzen in Systemen ohne domänenübergreifende Kommunikation folgt nun der Ausbau in der E/E-Architektur über Domänengrenzen hinweg. Das wirft Fragen zu Security, Safety und zuverlässigem Zeitverhalten auf. Praktikable Ethernet-Lösungen sind gefragt.



Einordnung der verschiedenen sicherheitsrelevanten Protokolle (grün).

Die Datenraten im Automobil steigen rasant. Um sie bewältigen zu können, bekommen klassische Bussysteme wie CAN und FlexRay Gesellschaft: Ethernet. Was im Infotainment-Bereich begann, setzt sich mittlerweile in domänenübergreifenden Systemen fort.
Für ein sicheres Neben- und Miteinander der Datenbusse sind durchdachte Lösungen gefragt. Neben der Kommunikation der Ethernet-Komponenten untereinander ist der reibungslose Datenaustausch mit den konventionellen Bussystemen zu gewährleisten. Zudem gilt es, Ethernet-Standards – wo nötig – den fahrzeugspezifischen Anforderungen anzupassen. Teils lassen sich Lösungen aus der klassischen IT übertragen oder nach geringfügiger Modifikation implementieren. Teils sind neue Entwicklungen nötig. Die Entscheidung darüber steht und fällt mit der Frage, wie ein Höchstmaß an Security, Safety und ein zuverlässiges Zeitverhalten, auch in Anbetracht großer Datenmengen wie bei Videosignalen, zu erreichen ist.

Probleme und Lösungen der klassischen IT

Im dezentralen Aufbau von Ethernet lässt sich mithilfe eingebauter Redundanzen und der Nutzung dynamischer Netzwerkpfade eine zentrale Kontrollinstanz vermeiden – und somit ein Single Point of Failure. Doch eben dieser verteilte Aufbau sorgt für Zweifel: Wenn alle Mitglieder in Ethernet-Netzwerken gleichberechtigt sind, wie können unerwünschte Netzwerkteilnehmer erkannt und verbannt werden? Wie werden Manipulationen am Netzwerk festgestellt und verhindert?
Dafür gibt es etablierte Lösungen. Etwa virtuelle Netzwerke, sogenannte VLANs, zur Trennung des Netzwerk-Traffics. Ursprünglich wurden die Netzwerk-Ports der verbauten Switches verschiedenen VLANs zugewiesen. Mittlerweile ist es auch möglich, Ethernet-Frames und Port-unabhängige VLANs zu markieren. Dieses „Taggen" ist im Standard IEEE 802.1Q definiert.
Die logische Trennung von Netzwerkverkehr allein verhindert aber nicht die Teilnahme unerwünschter Geräte. Auch schützt sie den Traffic nur bedingt vor Manipulation und Ausspähung. Dafür braucht es kryptografische Authentisierung oder Verschlüsselung. Auch hierfür sind Lösungen in der klassischen IT etabliert: Was auf den oberen Protokollschichten mit Datenformaten und Standards wie Transport Layer Security (TLS) begann, wurde später durch Sicherheitsmechanismen für die tieferen Layer ergänzt. Dazu zählen die Verschlüsselung von IP-Paketen (Layer 3) durch IPsec und von Ethernet-Frames (Layer 2) per MACsec (IEEE 802.1AE). Es handelt sich ebenfalls um standardisierte Lösungen.
Hinzukommen Sicherheitskomponenten: Klassische Firewalls kontrollieren anhand von Filterregeln, welche Pakete zwischen verschiedenen Netzen oder Endpunkten erlaubt sind. Moderne Varianten können den Traffic mittels Deep Packet Inspection bis hin zu den Nutzdaten der Pakete analysieren und bewerten. Darauf bauen wiederum Intrusion-Detection- bzw. -Prevention-Systeme (IDS bzw. IPS) auf – und erweitern die Kontrollmöglichkeiten der Administratoren.

Sicherheitsanforderungen moderner Fahrzeugnetzwerke

Netzwerkarchitekturen moderner Fahrzeuge und in der klassischen IT haben viele Parallelen. Doch die technischen Randbedingungen und Schutzziele unterscheiden sich teils deutlich. Im Fahrzeug hat das Abwenden von Schaden an Mensch und Maschine oberste Priorität. Das rückt die Authentizität des Netzwerkverkehrs und die Systemverfügbarkeit in den Fokus. Dort finden sich zudem die hohen Echtzeitanforderungen im Fahrzeugbetrieb: Nahezu verzögerungsfreies, deterministisches Verhalten der Netzwerkkomponenten wird voraussetzt.
Diese Erfordernisse stehen vermeintlich im Widerspruch dazu, dass Ethernet als paketbasiertes Best-Effort-Medium keine harten Garantien für die Zustelldauer von Datenpaketen kennt. Zusätzlich wird das Erfüllen der Schutzziele und Echtzeitanforderungen dadurch erschwert, dass in Fahrzeugen meist eher Komponenten mit limitierter Rechenleistung verbaut werden. Aus diesen Gründen finden etablierte Sicherheitstechnologien häufig nur in abgewandelter Form den Weg in Fahrzeugnetzwerke. Etwa, wenn VLANs zur Erhöhung der Ausfallsicherheit genutzt werden. Das Netzwerk wird dazu in virtuelle Zonen mit unterschiedlichem Schutzbedarf eingeteilt, über die der Netzwerkverkehr sicherheitsrelevanter Komponenten in Echtzeit identifizierbar wird. Bei Bedarf kann er so priorisiert und isoliert werden. Fluten beispielsweise ein Denial-of-Service-Angriff oder eine fehlerhafte Komponente das Netzwerk mit Paketen, lassen sich diese am nächsten Switch per Rate Limiting aufhalten, um der Kommunikation im priorisierten VLAN Vorrang zu geben.
Mithilfe von Firewalls oder leistungsfähigeren IDS-/IPS-Systemen lassen sich angrenzende IP-Netze mit unterschiedlichem Schutzbedarf noch schärfer voneinander trennen und genauer überwachen. Dagegen erlauben klassische Automotive-Bussysteme als Broadcast-Medium an sich keine logische Trennung – es sei denn, es wird ein zusätzlicher physikalischer Bus verbaut.

Bestehende und neue Security-Lösungen

Vorsicht war bisher beim etablierten IT-Sicherheitsprotokoll TLS geboten. Da hier Konflikte mit den Echtzeitanforderungen im Fahrzeug drohten, kamen sie nur für die zeitlich unkritische Kommunikation mit Backend-Systemen oder Testgeräten infrage. TLS 1.3 bringt hier substanzielle Neuerungen: Dank der Optimierung im Verbindungsaufbau (Zero-RTT Handshakes) lassen sich TLS-gesicherte Daten bereits im Handshake im ersten Paket unterbringen. Zusätzliche Paketumlaufzeiten bzw. Round Trip Times (RTTs) beim TLS-Einsatz entfallen. Da durch den Einsatz von Pre-Shared Keys (TLS-PSK) obendrein asymmetrische Verfahren verzichtbar werden, lässt sich der Overhead von TLS dramatisch reduzieren. Noch gilt es jedoch, die Möglichkeiten mit Blick auf die mögliche Abschwächung der TLS-Sicherheitsgarantien sorgfältig zu evaluieren.
Die Echtzeitanforderungen im Automobil stehen dem Einsatz kryptografischer Signaturen auf Basis asymmetrischer Verfahren entgegen. Zum Schutz der Authentizität von Datenpaketen wurde daher 2014 das Secure-On-board-Communication-Modul (SecOC) als Teil von AUTOSAR 4.2 spezifiziert. Die Spezifikation ist so flexibel, dass sich SecOC auch für den Ethernet-/IP-basierten Verkehr eignet.
Gleiches gilt für diverse Standards des Time-Sensitive Networking (TSN). Darunter das ursprünglich für die Übertragung zeitkritischer Videodaten entwickelte Audio Video Bridging (AVB). Es setzt auf Ethernet auf und definiert eigene Mechanismen, die die Reservierung von Netzwerkressourcen, die Synchronisierung von Zeitsignalen oder die Priorisierung von Datenströmen regeln. Zudem erlaubt AVB die Übertragung konventioneller Busdaten. Das trägt den Anforderungen in Umgebungen mit Echtzeitanforderung Rechnung, ohne auf Ethernet als Basistechnologie zu verzichten. Die neueste Fassung des AVB-Transportprotokolls (Ende 2016) unterstützt zudem optional die Verschlüsselung übertragener Nutzdaten – mit vergleichsweise geringen Hardware-Anforderungen.

Ethernet-Security im Fahrzeug – Entwicklung und Integration

Die Integration von Ethernet-basierten Lösungen in Fahrzeugnetzwerke ist in vollem Gange. Der Standard macht die Funktionen möglich, die von künftigen Fahrzeugen erwartet werden. Dabei steht die Entwicklung keineswegs im Widerspruch zu den Sicherheitsanforderungen im Automobil. Mit sachkundiger Begleitung durch Security-Experten und passgenauen Sicherheitslösungen gelingt die Implementierung sicherer Ethernet-Architekturen trotz aller Komplexität. ESCRYPT kann hierfür auf langjährige Erfahrungen im Ethernet-Security- wie im Automotive-Bereich zurückgreifen. Mit diesem Know-how werden Kunden in allen Phasen der Ethernet-Integration unterstützt: Von der Erarbeitung tragfähiger Sicherheitskonzepte und -analysen bis zur individuellen Implementierung von Soft- und Hardwarelösungen aus einem breiten, exakt auf die Automobilindustrie zugeschnittenen Portfolio. Abgesichert durch intelligente Security-Lösungen und -Produkte wird der Ethernet-Standard seine über 40-jährige Erfolgsgeschichte fortschreiben – auch und erst recht in der Automobilindustrie.

Immunsystem für das vernetzte Fahrzeug

Schutz durch Intrusion Detection and Prevention System (IDPS)

Mehr Sicherheit und Komfort. Optimierter Service und kurzweiligere Autofahrten. Die Liste der Vorteile von vernetzten Fahrzeugen ist lang. Doch die Einbindung ins Internet der Dinge birgt auch Risiken. So steigt die Gefahr von Cyber-Attacken. Angreifer finden immer neue Angriffspunkte. Darum brauchen vernetzte Fahrzeuge lernende Abwehrsysteme. Diese erkennen Angriffe auch dann, wenn das Muster noch unbekannt ist und können neue Erfahrungen zügig an andere Fahrzeuge im Feld weitergeben.

AUTOR

Dr. Jan Holle ist Security Engineer und Produktmanager bei der **ESCRYPT GmbH**.

ESCRYPT ist eine hundertprozentige Tochtergesellschaft von ETAS und bietet Sicherheitslösungen im Bereich Embedded Security an.

Sind Fahrzeuge in Kundenhand, dann haben Hersteller nur punktuell Zugriff auf deren Systeme. Dennoch erwarten Käufer zurecht, dass ihre Fahrzeuge jederzeit sicher sind. In Zeiten zunehmend vernetzter Fahrzeuge tut sich damit eine neue Herausforderung auf. Zwar erhalten die Hersteller bessere Zugriffsmöglichkeiten, doch steigt mit der Einbindung ins Internet der Dinge auch das Risiko unbefugter Zugriffe und böswilliger Cyber-Attacken.

Funktionale Sicherheit (Safety) allein reicht nicht mehr. Hersteller müssen auch umfassende IT-Sicherheit (Automotive Security) garantieren, wenn hunderte Millionen vernetzte Fahrzeuge in aller Welt unterwegs sind. Hinzukommt der Trend zum automatisierten Fahren, der die Sicherheitsanforderungen an IT-Systeme weiter erhöht.

Holistischer Schutz über den Gesamtlebenszyklus hinweg

Um das nötige Sicherheitsniveau zu erreichen, bedarf es durchdachter und sauber implementierter Maßnahmen. Automotive Security ist nicht – oder nur zu horrenden Kosten – nachrüstbar. Gefragt sind vielmehr holistische Strategien, in denen Safety und Security von Tag eins der Entwicklung an zusammen betrachtet werden. Standardisierte Prozesse in der Entwicklung von Embedded Software gehören ebenso dazu wie zuverlässige Schutzvorkehrungen. Moderne Chip-Architekturen mit Hardware-Security-Erweiterungen – darunter Hardware-Security-Module und Secure-Hardware-Extensions – schirmen sicherheitsrelevante Systembereiche physikalisch gegen unbefugte Zugriffe ab. Rund um diese Sicherheitskerne sind weitere Maßnahmen nötig: Secure-Boot-Funktionen, die etwaige Manipulationen an der Steuergeräte-Firmware erkennen, sowie geschützte Netzwerkübergänge (Gateways) oder kryptografische Lösungen zur Absicherung sämtlicher Kommunikation. Nicht minder wichtig sind organisatorische Schutzmaßnahmen in der Entwicklung und Produktion, von zugangsbeschränkten Sicherheitsbereichen bis hin zur Begrenzung der Zugriffsrechte auf Krypto-Schlüssel und Freischaltcodes auf einige wenige Verantwortliche. Die beschriebenen Maßnahmen senken die Wahrscheinlichkeit von zufälligen Fehlern. Und sie erhöhen den Aufwand für Hacker, in Fahrzeugsysteme einzudringen. Doch sie beantworten noch nicht die Frage, wie der Schutz vernetzter Systeme zu gewährleisten ist, sobald das Fahrzeug in Kundenhand ist. Denn in dieser Kernphase des Lebenszyklus bleiben die Zugriffsmöglichkeiten für Hersteller begrenzt. Sie müssen die Fahrzeugsysteme theoretisch während der Entwicklung für Angriffe wappnen, die über ein Jahrzehnt in der Zukunft liegen können. Ein Rückblick auf den Stand der Informationstechnologie vor zehn Jahren genügt, um zu verstehen, dass dies kaum möglich sein wird.

Die Herausforderung: Schutz vor unbekannten Gefahren

Daraus folgt: Die Maßnahmen der IT-Sicherheit müssen dynamisch und fortlaufend sein, um die Systeme auch in Kundenhand zuverlässig zu schützen. Doch während die Randbedingungen der funktionalen Sicherheit meist auf Naturgesetzen und statistischen Vorhersagen beruhen, die im Betrieb weiter gelten, sind die Annahmen und Randbedingungen der IT-Sicherheit volatil. Denn Angreifer suchen immer neue Schwachstellen im System. Es liegt in der Natur der Sache, dass die Hersteller in der Regel nicht um die Existenz dieser Schwachstellen wissen. Ebenso wenig können Security-Experten alle Angriffsstrategien vorhersehen, die viele Jahre in der Zukunft liegen. Auch die klassische IT steht vor der Aufgabe, IT-Infrastrukturen vor An-

griffen mit unbekanntem Muster zu schützen. Hier versuchen Angreifer, Sicherheitsmechanismen auszuhebeln, die als sicher gelten.
Schutz bieten hier immer öfter sogenannte intelligente Angriffserkennungs- und Abwehrsysteme (Intrusion Detection and Prevention Systems, IDPS). Bei näherer Betrachtung erscheinen diese Systeme dafür prädestiniert, auch das vernetzte Fahrzeug zu schützen.

Immunisierung per IDPS

Das Besondere an der IDPS-Technologie: Sie nutzt die Vernetzung der Fahrzeuge, um schnell auf neue Angriffsszenarien reagieren zu können und um die daraus resultierenden Abwehrstrategien umgehend an die gesamte Fahrzeugflotte weiterzugeben. So entsteht eine Art Immunsystem, das dynamisch auf Angriffe reagiert – und in dem jeder Angriff die Abwehrkräfte der Flotte stärkt. Kern des IDPS von ESCRYPT ist eine spezielle Security-Software. Sie wacht in Steuergeräten oder Gateways und analysiert permanent die komplette Bordnetzkommunikation. Tauchen Anomalien auf, dokumentiert sie diese – und leitet im Ernstfall die Abwehr ein. Ist das erkannte Angriffsmuster schon bekannt, blockieren Firewall-Mechanismen die Kommunikation zwischen den verschiedenen Datenbussen. Dies ist bereits Routine – und wie das gesamte IDPS auf heute gängige CAN- sowie auf künftige Ethernet-Netzwerke anwendbar. Die IDPS-Technologie ist aber vor allem in der Lage, unbekannte Muster und Angriffsstrategien zu erkennen und zu parieren. Dafür verfügt sie über hinterlegte Regelsets (Black-/Whitelists), die ständig aktualisiert werden. Genau hier liegt eine Stärke des Ansatzes: Anomalien und Anzeichen für bisher noch unbekannte Attacken werden von der Angriffserkennungssoftware CycurIDS detektiert. Sie kann erkannte Anomalien im Fahrzeug speichern, damit sie später auslesbar sind. Wirksamer ist aber eine Funktion, die alle Anomalien automatisch in eine cloudbasierte Eventdatenbank übermittelt. Hier laufen sämtliche Auffälligkeiten aus allen vernetzten Fahrzeugen des Herstellers mit den Fingerprints bekannter Attacken zusammen und können abgeglichen werden.

Gesamtflotte als Basis für dynamische Schutzstrategie

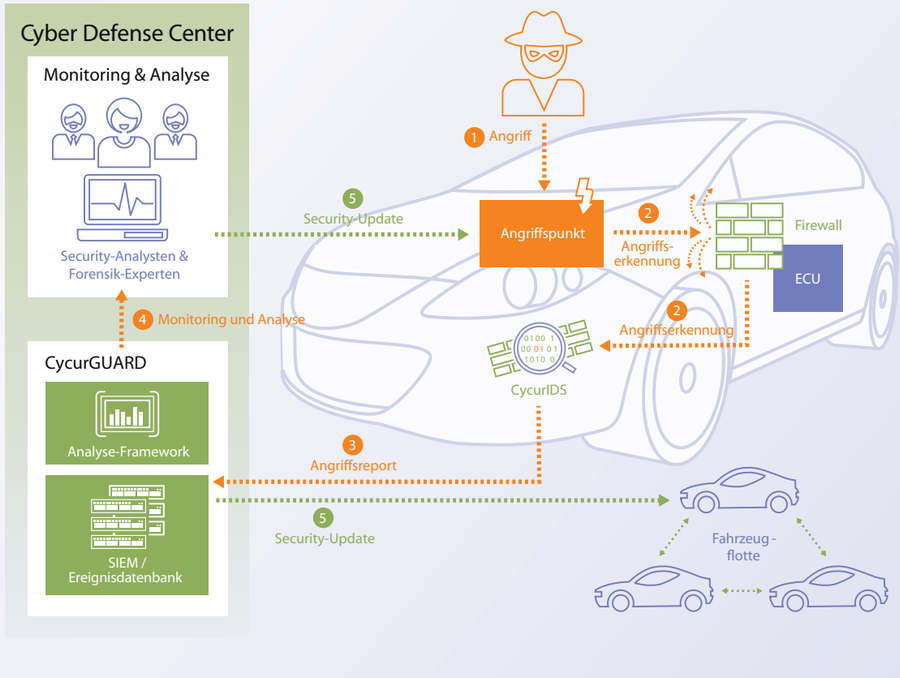
Aus der Analyse der Daten bekommen OEMs einen umfassenden, jederzeit aktuellen Überblick darüber, welche Strategien Hacker verfolgen, welche Angriffspunkte sie anvisieren und ob sich Attacken häufen. Zur Auswertung dieser umfassenden Eventdatenbasis in einem Backend greift die nächste Stufe des dynamischen Abwehrsystems: Die automatisierte, auf Big-Data-Methoden basierende Softwarelösung Cycur-GUARD. Diese analysiert die Angriffsmuster und nimmt eine Vorsortierung vor, anhand derer Sicherheitsexperten und Security-Forensiker in einem Cyber Defense Center entscheiden, ob und welche Gegenmaßnahmen einzuleiten sind. Dazu zählen gezielte Anpassungen der Firewall, Updates des CycurIDS-Regelsets – oder die Beseitigung von Schwachstellen in der Software betroffener Steuergeräte in enger Abstimmung mit deren Herstellern. Die getroffenen Maßnahmen können dann „Over-the-Air“ an alle vernetzten Fahrzeuge der Flotte übermittelt werden – selbstverständlich kryptografisch abgesichert. Zusätzlich sind die Updates durch digitale Signaturen vor unbemerkten Veränderungen geschützt.

Fazit

Weil sämtliche erkannten Anomalien aus allen Fahrzeugen im Feld in der zentralen cloudbasierten Eventdatenbank zusammenlaufen, fallen neue Angriffsmuster schnell auf. Mit jedem Fahrzeug, das diesem Verbund angeschlossen ist, wird IDPS intelligenter und abwehrfähiger. Denn da bisher unsichtbare, gegebenenfalls von Firewalls abgeblockte Angriffe in eine ständige Lageauswertung einfließen, lassen sich Security-Maßnahmen schneller und gezielter an aktuelle Risiken anpassen. Im Verbund entsteht so ein Immunsystem für das vernetzte Fahrzeug, dessen Abwehrkräfte durch jeden Angriffsversuch gestärkt werden. Die stetig wachsende Datenbasis und sofortige Weitergabe der Abwehrstrategien an alle Fahrzeuge im Bestand gewährleisten immer umfassenderen Schutz.

Holistischer Schutz über den gesamten Lebenszyklus hinweg.

In fünf Schritten zur „immunisierten“ Flotte.



Embedded-Security-Tests im virtuellen Fahrzeug

Umfassende Angriffssimulationen mittels XiL-Testumgebung

Moderne softwaregesteuerte Fahrzeugsysteme müssen nicht mehr nur funktional sicher sein, sie brauchen auch Schutz gegen Angriffe von Cyberkriminellen. Um testen zu können, ob angegriffene Steuergeräte im Kontext des Gesamtfahrzeugs sicher bleiben, setzen ETAS und ESCRYPT auf Virtualisierung. Die Vorteile der XiL*-Technologie werden so auch für Security-Tests nutzbar.

AUTOREN

Jürgen Crepin ist Senior Expert Marketingkommunikation bei der **ETAS GmbH**.

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

Ein Albtraum: Hacker verschaffen sich Zugriff aufs Fahrzeugsystem, fangen Sensorsignale ab, speisen stattdessen korrumpierte Daten in Steuergeräteschnittstellen ein. Aus heiterem Himmel wäre der Fahrer machtlos, säße im fremdgesteuerten Fahrzeug. Damit solche Szenarien fiktional bleiben, sind verlässliche Security-Lösungen gefragt.

Doch lassen sich Hackerangriffe testen? Oder präziser: Lässt sich der Nachweis führen, dass Security-Maßnahmen Fahrzeugsysteme zuverlässig abschirmen? Im Bereich der funktionalen Sicherheit sind Hardware-in-the-Loop-(HiL-)Systeme etabliert, um nachzuweisen, dass Funktionen im Normalbetrieb und bei Störungen wie geplant reagieren. Dabei testen Entwickler die Software sowie die Interaktion verteilter Sensorsysteme und Fahrzeugdomänen in Simulationen ganzer Fahrzeuge inklusive aller Steuergeräte und Datennetze. Echtzeit-HiL-Systeme wie ETAS LABCAR, die Co-Simulationslösung ETAS COSYM oder virtuelle, per ETAS ISOLAR-EVE erzeugte Steuergeräte bieten dafür die technologische Basis.

Neue Option: Security-in-the-Loop

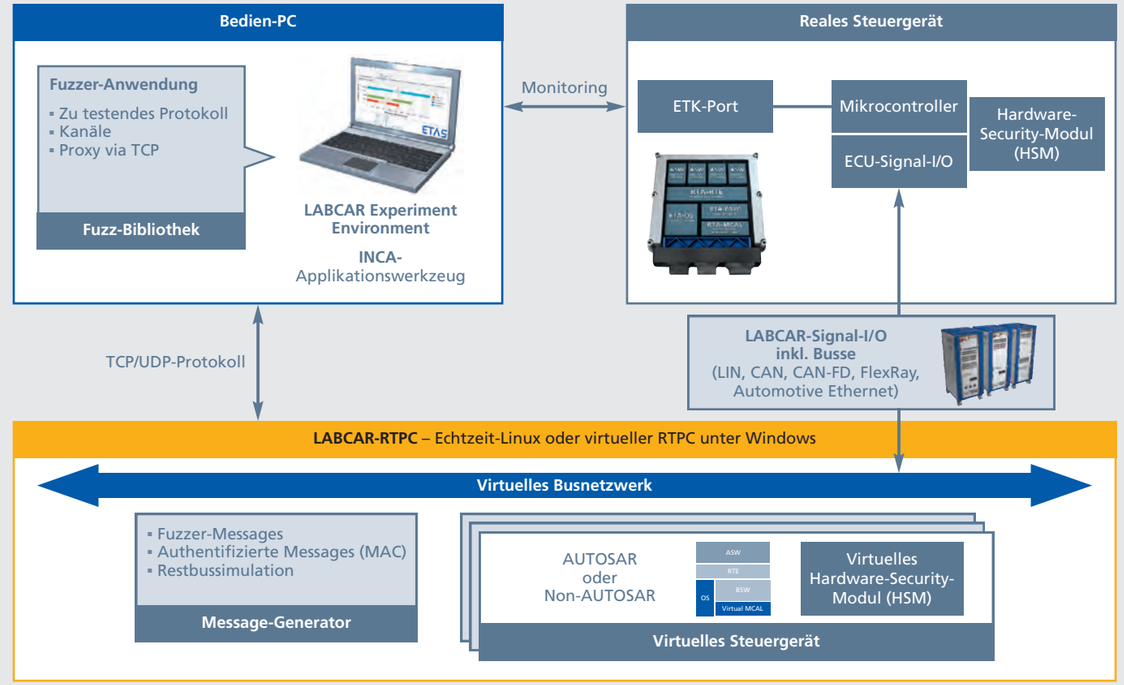
Für Security-Tests ist die True-Positive-Methode, also das Abprüfen eines erwarteten Verhaltens, wenig effektiv, da die Angriffsszenarien zum Zeitpunkt der Entwicklung in der Regel unbekannt sind bzw. bekannte Sicherheitslücken direkt geschlossen werden. Stattdessen gilt es, die Suche nach Schwachstellen zu systematisieren. Auch dafür eignen sich Software-in-the-Loop-(SiL-) oder HiL-Testumgebungen.

Die Herausforderung hierbei besteht darin, Kompetenzen aus unterschiedlichen Domänen zu vereinen: Security-Experten müssen sich mit der XiL-Test-Methodik und XiL-Testingenieure mit Methoden aus dem traditionellen IT-Umfeld vertraut machen, die nun zur Identifikation potenzieller Schwachstellen im eingebetteten System genutzt werden. Da hierbei vor allem sicherheitsrelevante Fahrzeugfunktionen im Fokus stehen, müssen derartige Security-Tests von Anfang an konsequent geplant und effizient ausgeführt werden.

ETAS und ESCRYPT haben diese Herausforderung früh erkannt und ihr Know-how aus den Bereichen Safety, XiL-Verfahren sowie Automotive Security zusammengeführt. Das Ergebnis ist eine Lösung, die das Beste beider Welten verbindet (siehe Grafik). Ein virtuelles Testfeld auf Basis der LABCAR-Hardware, dem Linux-basierten Simulationstarget LABCAR-RTPC (Real-Time-PC) und der virtuellen Steuergeräte-Lösung ISOLAR-EVE ermöglicht es, Angriffe auf einzelne Steuergeräteschnittstellen sowie Manipulationsversuche an Steuergerätefunktionen im Kontext des Gesamtfahrzeugs zu simulieren.

LABCAR für Security-Tests

Während ETAS für das Testsystem verantwortlich ist, bringt ESCRYPT die Security-Expertise bei der Auswahl sinnvoller Testverfahren ein – beispielsweise:



Prinzipieller Aufbau eines Security-Testsystems.

▪ **Penetration-(PEN-)Testing**, bei dem der Tester versuchen, das Verhalten von Steuergeräten von außen (zum Teil auch durch mechanischen Eingriff) zu verändern, unbefugt Daten auszulesen oder das eingebettete System zu beschädigen. Das teilautomatisierte „PEN-Testing-in-the-Loop" von ETAS und ESCRYPT nutzt für optimale Testabdeckung eine Angriffsbibliothek, die durch Erfahrungen aus ESCRYPT Consulting-Projekten kontinuierlich erweitert wird.

▪ **Fuzz-Testing**, bei dem eine Testsoftware – der „Fuzzer" – automatisiert zufällige Inhalte („Dumb Fuzzing") oder gezielt manipulierte Befehle und Signale generiert, mit denen er Steuergeräte-Ports flutet. Um Einbruchsversuche oder Manipulationen durch Hacker zu simulieren, fließt in der Regel für effizienteres Testen Wissen über das Protokoll, das Softwaresystem und die Krypto-Absicherung getesteter Steuergeräte in die Signalgenerierung mit ein.

▪ **Message-Authentification-(MAC-)Testing**, mit dem geprüft wird, ob wirklich nur unveränderte Botschaften von befugten Absendern Eingang in die Systeme finden. Dafür bietet das Testsystem die Möglichkeit zur Generierung kryptografischer Schlüssel und Zähler sowie Mechanismen für deren Interpretation im Rahmen der Decodierung. Anhand der Reaktionen einzelner und mehrerer Steuergeräte im Verbund lassen sich mit den Tests Schwachstellen in der Fahrzeug-IT systematisch aufdecken. Theoretisch gibt es eine nahezu unendliche Zahl an Testvektoren. Darum gilt es, Testfälle sinnvoll einzugrenzen. ETAS und ESCRYPT belassen es genau deshalb nicht bei der Bereitstellung von Simulations- und Testwerkzeugen – sondern bieten kompetente Beratung beim Erstellen der Testpläne und Konfigurieren der LABCAR-Testumgebung.

Die XiL-Technologie und Werkzeuge für Steuergerätezugriff (zum Beispiel ETK) von ETAS sind die Voraussetzung für umfassende Security-Tests: Tester haben vollen, zeitsynchronen Zugriff auf Speicher und interne Datenverarbeitung getesteter Steuergeräte und können deren Funktionen und Prozesse im Zuge der PEN-, Fuzz- und MAC-Tests exakt nachvollziehen. Erst diese Echtzeitmechanismen und erweiterten Monitoring-Funktionen ermöglichen Analysen in der nötigen Breite und Tiefe.

Fazit

ETAS und ESCRYPT haben über viele Jahre hinweg Kompetenzen in den Bereichen Automotive Security und XiL-basiertes Testen aufgebaut. Diese Kompetenzen wachsen nun zusammen, um Steuergeräte-Netzwerke rundum abzusichern. Bei Verwendung sinnvoller Testverfahren sind XiL-Systeme bestens geeignet, um Security-Mechanismen zu verifizieren und Sicherheitslücken aufzudecken. Damit ist ein weiterer wichtiger Schritt auf dem Weg zum sicher vernetzten Fahrzeug der Zukunft getan.

Welche Möglichkeiten das Testing-Labor von ESCRYPT bietet, erfahren Sie auf der nächsten Seite.

* XiL = Model-, Software- und Hardware-in-the-Loop (MiL, SiL, HiL)

Von A bis Z durchgetestet

Security-Tests für den gesamten Fahrzeuglebenszyklus

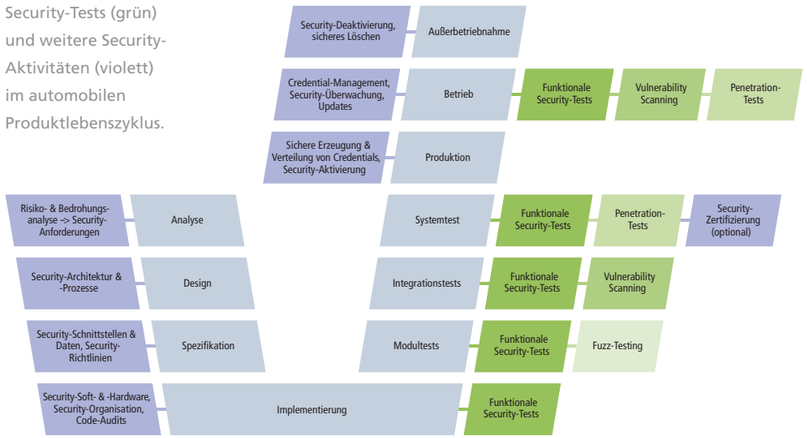
AUTOREN

Dr. Markus Kögel ist Expert Security Consultant bei der **ESCRYPT GmbH**.

Dr.-Ing. Marko Wolf ist Head of Consulting und Engineering bei der **ESCRYPT GmbH**.

ESCRYPT ist eine hundertprozentige Tochtergesellschaft von ETAS und bietet Sicherheitslösungen im Bereich Embedded Security an.

Wirkungsvolle Informationssicherheit erfordert Security-Tests während des gesamten Fahrzeuglebenszyklus. Denn im Gegensatz zu klassischen Tests zur Fahrsicherheit, bei denen sich die meist durch physikalische Gesetzmäßigkeiten bestimmten Randbedingungen später nicht mehr ändern, unterliegen die Annahmen und Randbedingungen der Security-Tests dem ewigen Wettstreit zwischen Angreifer und Verteidiger. Deshalb sind auch nach Produktionsstart bis zur Außerbetriebnahme des Fahrzeugs regelmäßige Security-Tests notwendig, um auch neu entwickelte Cyberangriffe und bisher unentdeckte Sicherheitslücken zu prüfen und notfalls noch effektiv darauf reagieren zu können.



Security-Tests (grün) und weitere Security-Aktivitäten (violett) im automobilen Produktlebenszyklus.

Automotive-Security-Testmethoden für jede Phase

Die Security-Tests im Automobilbereich (Automotive Security Testing) unterscheiden im Wesentlichen vier verschiedene Testmethoden, die im erweiterten V-Modell der aufsteigenden Flanke verortet sind (siehe Grafik), konkret: funktionale Security-Tests (Functional Security Testing), automatisierte Schwachstellensuche (Vulnerability Scanning), Fuzz-Testing (Fuzzing) und sogenannte Penetration-Tests. In all diesen Bereichen bietet ESCRYPT umfangreiche Beratung und Dienstleistung an.

Funktionale Security-Tests werden eingesetzt, um zu prüfen, ob die Spezifikation der verwendeten Security-Mechanismen korrekt und vollständig umgesetzt wurde. Das Vorgehen ist sehr ähnlich zu klassischen funktionalen Tests, der Fokus wird hier allerdings auf die Security-Funktionalität gelegt. Dabei wird sowohl die Implementierung – beispielsweise von Verschlüsselungs- oder Authentifizierungsalgorithmen – auf Fehlerfreiheit getestet als auch die Performance und der Ressourcenverbrauch der Implementierung betrachtet, um zum Beispiel mögliche Konflikte mit Laufzeitanforderungen oder Speicherbedarfen zu identifizieren.

Fuzzing-Tests werden zusätzlich zu den funktionalen Security-Tests angewendet, um systematisch durch verschiedene unerwartete, ungültige oder unplausible Nachrichten ein instabiles oder gar fehlerhaftes Verhalten des Systems aufzudecken.

Vulnerability Scanning wiederum konzentriert sich auf die umfängliche Prüfung bereits bekannter Einfallstore, Sicherheitslücken und Verwundbarkeiten für Cyberangriffe. Für diese Security-Tests wird meist eine stetig aktualisierte Datenbank mit allen zu dem Zeitpunkt bekannten Schwachstellen für das Testobjekt verwendet.

Penetration-Tests untersuchen in der Regel erst die Release-Kandidaten von neuen Automotive-IT-Systemen. Diese erweiterten Security-Tests folgen dem Prinzip, dass ein IT-System nur dann ausreichend getestet ist, wenn es auch mit dem Wissen, Können und den Werkzeugen eines realistischen Angreifers umfangreich untersucht wurde.

ETAS und ESCRYPT bieten hier neben Beratung und Dienstleistung verschiedene Testsysteme an (siehe S. 12). Insbesondere ESCRYPT führt seit über einem Jahrzehnt Security-Tests für Automotive-Security-Anwendungen durch und ist Partner vieler OEMs und Zulieferer. Das ETAS-Tochterunternehmen verfügt über ein hochmodernes Testing-Labor und ist für diverse Angriffsmethoden bestens gerüstet – ganz gleich ob PEN-Testing von Hardware, Software oder Automotive-Netzwerken.

Neu ist ASCET nicht. Die ersten sechs Generationen des ETAS-Tools haben sich in der Software-Entwicklung für mehr als 450 Millionen Steuergeräte bewährt. Dennoch hat ETAS die siebte Generation, den ASCET-DEVELOPER 7, gründlich überarbeitet und so fit für die Zukunft gemacht.

Die Ziele waren anspruchsvoll: höhere Produktivität, noch bessere Absicherung gegen Programmierfehler, volle Konformität mit Industriestandards sowie die reibungslose Einbettung in die Entwicklungslandschaften der Kunden. Gelungen ist das durch die Integration in die offene Entwicklungsplattform Eclipse, die Konformität mit Standards, wie MISRA-C:2012, IEC 61508 und ISO 26262, neue Ideen für noch mehr Sicherheit und eine deutlich bessere Benutzerführung.

On-the-Fly-Überprüfung gibt den Ingenieuren Sicherheit

Doch wie lässt sich Embedded Software, die in immer komplexeren Systemen sicherheitsrelevante Funktionen steuert, zugleich kostengünstig und sicher programmieren?

Die Antworten auf diese Frage lauten Embedded Software Development Language (siehe Seite 16) und höherer Automatisierungsgrad. Der Verzicht auf ermüdende manuelle Dateneingabe legt typische Fehlerquellen trocken: Syntax- und Typisierungsfehler, verrutschte Kommata oder falsche Einheiten. Eine On-the-Fly-Prüfung aller Eingaben deckt auch jene Fehler auf, die in statischen Analysen durch die Raster fallen: ob Division durch Null, Unter- und Überlauf oder überschrittene Indexgrenzen bei Arrays. Der Entwickler erhält sofort Rückmeldung und kann den Fehler gleich beseitigen.

ASCET-DEVELOPER 7 beugt durch die systematischen Prüfungen teuren Fehlern vor. Die Modelle sind für Open-/Closed-Loop-Simulationen und für das Prototyping nutzbar. Am Ende steht automatisch erzeugter, abgesicherter C-Code für die weiteren Prozessschritte zur Verfügung.

Fazit: sicherer und produktiver

Feldtests bei Kunden belegen: Dank des systematischen Ausräumens von Fehlerquellen und der Automatisierung gelingt die Modellerstellung mit ASCET-DEVELOPER 7 doppelt so schnell wie mit der Vorgängerversion ASCET 6. Das steigert die Produktivität. Und die verbesserte Kompatibilität, Portabilität sowie die Konformität mit höchsten Sicherheitsstandards geben Software-Ingenieuren das gute Gefühl, auf einen reibungslosen, rundum abgesicherten Workflow zu bauen.

AUTOR

Dr. Darren Buttle ist Produktmanager ASCET bei der **ETAS GmbH**.

Safety und Security im Code

AUTOR

Dr. Darren Buttle ist Produktmanager ASCET bei der **ETAS GmbH**.

ESDL als Basis für sichere Software

Für Embedded Software ist die Programmiersprache C das Maß der Dinge. Aber die Erstellung von sicherem C-Code ist nicht einfach. Doch je autonomer die Fahrzeuge werden, umso größer werden die Anforderungen an die Integrität der Software. Darum hat ETAS die Embedded Software Development Language (ESDL) entwickelt. Damit schaffen es Entwickler, mehr Software schneller zu entwickeln, die unter anderem die Standards ISO 26262 und IEC 61508 erfüllt.

In den letzten 40 Jahren hat sich C zur De-facto-Programmiersprache für die Entwicklung eingebetteter Software entwickelt. C ist einfach, kompakt, schnell, portabel und wird von vielen Tools unterstützt.

Doch C hat auch Tücken. Allzu leicht schleichen sich Fehler ein, die im Code nur schwer zu finden sind. Die Syntax macht es leicht, Fehler beim Programmieren zu machen – optionale Klammern, Zuweisungen in Ausdrücken und automatisches „switch/case-Durchfallen“ sind nur einige Beispiele. Zusätzlich gibt es semantisch zweifelhafte oder komplexe Features, die nur schwer richtig zu verwenden sind und dazu verleiten, „an der Grenze zur Sicherheit“ zu programmieren, beispielsweise Sprünge, Zeiger und integrale Promotion. Auch diese Aspekte können gefährlich zusammenwirken.

Durch die Verwendung von Programmierrichtlinien wie MISRA-C und CERT-C können viele dieser Risiken vermieden werden. Aber selbst bei Einhaltung dieser Richtlinien können weiterhin Probleme auftreten. Richtlinien verhindern weder Laufzeitprobleme wie Speicherüberlauf noch numerische Probleme wie Überlauf oder Division durch Null. Richtlinien können auch keine unsinnigen Operationen erkennen, wenn beispielsweise eine Geschwindigkeit einen Grenzwert überschreitet, eine Temperatur unter den absoluten Tiefpunkt fällt oder versehentlich eine Entfernung zu einem Druck addiert wird. C ist nicht expressiv genug, um diese Informationen zu erfassen und kann diese folglich auch nicht überprüfen.

Um diese Probleme zu vermeiden, sind zusätzliche Maßnahmen erforderlich, zum Beispiel statische Analysen und Testläufe zur Fehlerbehebung. Das ist ineffizient. Viel besser wäre es, Fehler von Anfang an zu vermeiden, damit sie gar nicht erst beseitigt werden müssen.

Eine bessere Programmiersprache

Die ETAS-Antwort auf all diese Herausforderungen lautet Embedded Software Development Language (ESDL) – eine neue Programmiersprache zur effektiven Erstellung sicherer Software. ESDL vermeidet die typischen Fallstricke der C-Programmierung, erleichtert die Wiederverwendung von Software, vereinfacht die Wartung und unterstützt Variantenverwaltung. Mit ESDL können Entwickler sich wieder mehr auf ihre Kernaufgaben konzentrieren und müssen nicht mehr um die Unzulänglichkeiten von C herum programmieren.

C-Code mithilfe von Codegenerierung

Die effiziente Verwendung von ESDL wird durch ETAS ASCET-DEVELOPER 7 (siehe Seite 15), einer Eclipse-basierten integrierten Entwicklungsumgebung (IDE) und einem C-Codegenerator, ermöglicht.

Die IDE bietet moderne Bearbeitungsfeatures wie Sprachtemplates, Codevorschläge und Quick Fixes für Probleme. Dadurch ist ESDL auch für Anfänger leicht zu lernen. ASCET-DEVELOPER 7 prüft kontinuierlich auf ESDL-Programmierfehler, berechnet Qualitätsmetriken und weist auf Best Practices hin. Entwickler erhalten Feedback „on-the-fly“ bereits bei der Bearbeitung. Zwischen der Eingabe eines Codierfehlers und seinem Auffinden vergeht praktisch keine Zeit.

Der C-Codegenerator übersetzt ESDL in MISRA-konformen C-Code. ASCET-DEVELOPER 7 fügt automatisch defensive Codeüberprüfungen an den Stellen ein, an denen sie für die Laufzeitsicherheit erforderlich sind. Damit müssen diese nicht von Hand ergänzt und verwaltet werden. Der generierte C-Code lässt sich leicht in einen bestehenden C-basierten Entwicklungsprozess integrieren.

Programmiersprache gegen mögliche Fehler absichern

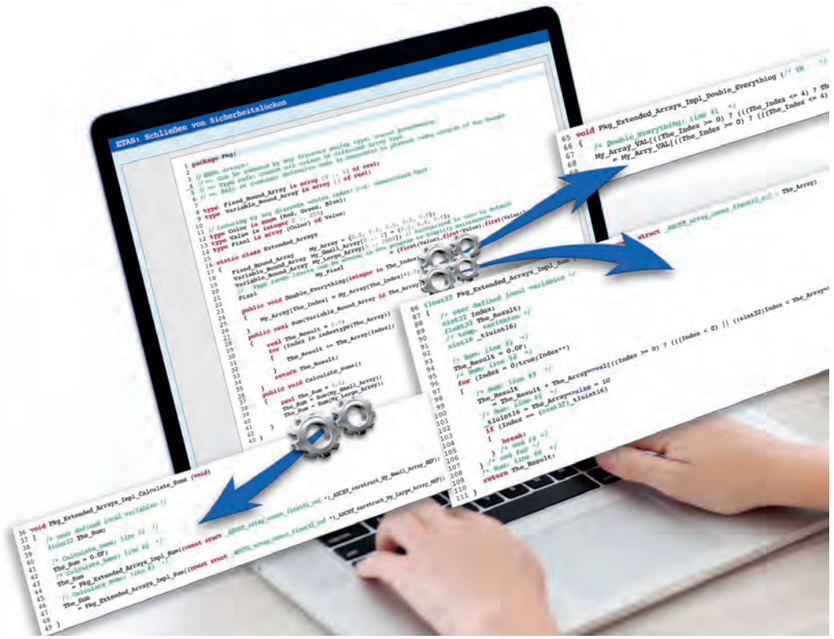
ESDL deckt viele Aspekte ab, die bereits in den C-Programmierrichtlinien enthalten sind. Zudem enthält das Design von ESDL Features, die es einfach machen, die Sprachanforderungen in Standards wie ISO 26262 und IEC 61508 zu erfüllen. Durch diese Konzepte in ESDL kann ASCET-DEVELOPER 7 mehr Fehlerfälle während der Bearbeitung überprüfen, als es in der klassischen C-Programmierung möglich ist.

Die ESDL-Syntax ist der von C sehr ähnlich, weshalb die Entwickler sich damit sofort vertraut fühlen. ESDL vermeidet jedoch die gefährlichen C-Features, die Richtlinien normalerweise einschränken oder verbieten. In ESDL gibt es keine optionalen Klammern, keine Anweisungen in Ausdrücken, keine Zuweisung an Schleifenvariablen, kein automatisches switch/case-Durchfallen, keine implizite integrale Promotion, keine globalen Variablen, keine Zeiger, keine Sprungfunktion, keine Unions usw. Das Fehlen all dieser Fallstricke macht ESDL schon in sich sicherer als C.

Alle ESDL-Berechnungen sind frei von numerischen Problemen wie Overflow, Underflow, Division durch Null oder Signed Overflow.

Array-Zugriffe außerhalb ihres Bereichs sind in ESDL nicht möglich: Das typische Pufferüberlaufproblem, bekannt aus vielen Sicherheitsberichten, kann mit ESDL nicht auftreten.

ESDL verfügt über ein umfangreiches Typsystem, welches einem Typen einen Namen zuweist (ähnlich wie



Sicherheitslücken können sofort beim Programmieren geschlossen werden.

ein „typedef" in C), aber mit weiteren Informationen zum zulässigen Wertebereich und (optional) zur erforderlichen Auflösung. In ESDL kann beispielsweise eine Geschwindigkeit als eine Fließkommazahl im Bereich von 0,0 bis 260,0 km/h mit einer Auflösung von 0,01 km/h definiert werden. Typen können Einheiten, zum Beispiel Meter, Grad oder Zeit, verwenden.

Die Kompatibilität der Einheiten wird automatisch überprüft und verhindert, dass beispielsweise eine Zeit zu einer Entfernung addiert wird.

Der Codegenerator von ASCET-DEVELOPER 7 verwendet die ESDL-Typeninformation, um den speicheroptimalen C-Typ auszuwählen und um defensive Code-Überprüfungen zur Laufzeit zu erstellen, welche die Plausibilität der Werte jederzeit sicherstellen.

Änderungen können leicht an einer Stelle im Programm vorgenommen werden und systematisch durch erneute C-Codegenerierung angewendet werden. Ein weiterer Vorteil: Reviews und Inspektionen sind mit ESDL einfacher. ESDL-Programme sind nicht überfrachtet mit händischen Bereichsüberprüfungen, die ein Programm unübersichtlich machen und ein einfaches Verstehen der Programmabläufe erschweren.

Datenzugriff kontrollieren und Wiederverwendung ermöglichen

ESDL ist objektbasiert und verwendet Klassen, um den Datenzugriff zu verwalten und zu kontrollieren. Objekte können sicher verwendet werden und verfügen über definierte Speicherbegrenzungen. Im Gegensatz zu C++ und Java gibt es bei ESDL keine Speicherlecks, weil auf eine dynamische Speicherzuweisung verzichtet wird.

Die ESDL-Klassen unterstützen auch Produktlinienvarianten, ohne dass „Clone & Own" von Funktionsverhalten erforderlich wäre. Varianten sind möglich für:

- Code
- Dateninitialisierung
- Speicherzuweisung
- C-Speicherdarstellung (zum Beispiel Wechsel zwischen Gleit- und Festkommadarstellung)

Die Datenkonsistenz in einer Echtzeitumgebung wird in ESDL über einen Thread-sicheren Kommunikationsmechanismus über „Messages" realisiert. Für diese werden Lese- und Schreibzugriffe klar definiert und damit ein unzulässiger Zugriff auf Daten verhindert.

Fazit

Im komplexen Entwicklungsumfeld zunehmend vernetzter Fahrzeuge kann die Flexibilität der Programmiersprache C zum Nachteil werden. Zu leicht schleichen sich unentdeckt Fehler in den Code ein und es ist zu zeitaufwendig und zu ineffizient, diese Fehler später im Entwicklungsprozess zu beheben. Bei der Arbeit mit C wird viel Zeit damit verbracht, die Fallstricke von C zu umgehen.

Mit ESDL und ASCET-DEVELOPER 7 ermöglicht ETAS es, sicheren C-Code effektiver und effizienter zu erstellen. ESDL beseitigt ganze Kategorien möglicher Fehlerquellen und erleichtert die Wiederverwendung von Software und generiertem Code über mehrere Projekte hinweg. Dank ESDL erreicht die Entwicklung von Embedded Software ein neues Niveau an Effizienz und Sicherheit.

Virtuelle Steuergeräte in Serienfahrzeugen?

AUTOREN

Michael Hauser ist Teamleiter Software-Entwicklung bei **Bosch Automotive Electronics** in Stuttgart.

Dr. James Dickie ist Produktmanager RTA-Solutions bei **ETAS Ltd** in York, Großbritannien.

Dr. Nigel Tracey ist General Manager bei **ETAS Ltd** in York, Großbritannien.

ETAS Lightweight Hypervisor sorgt für Flexibilität, Effizienz und Sicherheit

Die Automobilindustrie setzt zunehmend auf agile Software-Entwicklung. Bedenkenlos sollen Kunden softwaregesteuerte Fahrzeugfunktionen upgraden oder updaten können. Das setzt eine strikte Trennung der einzelnen Softwarefunktionen voraus. Der Trend bei der Hardware weist jedoch in die entgegengesetzte Richtung: Auf zentralen Steuergeräten laufen immer mehr Funktionen. Um diesen Widerspruch zu lösen, setzt Bosch Automotive Electronics den neuen Lightweight Hypervisor von ETAS ein.

Nach drei unfallfreien Jahren ist es so weit. Leons Eltern loggen sich beim OEM ein. Die softwaregesteuerte Leistungsdrosselung seines Autos, das er zum Führerschein bekommen hat, wird endlich entfernt. Zudem bekommt er das neue Multimedia-Paket aufgespielt, das er zur Hälfte selbst bezahlt.

Nachträgliche Funktionsupgrades und fortlaufende (Over-the-Air-)Updates setzen voraus, dass Modifikationen keinesfalls andere Software in Mitleidenschaft ziehen. Doch wie lässt sich das gewährleisten, wenn der Trend gleichzeitig zur Konzentration von immer mehr miteinander vernetzten Funktionen auf wenigen, zentralen Steuergeräten geht? Ist es in einem solchen Umfeld überhaupt möglich, vorab mit Tests die funktionale Sicherheit des Gesamtsystems nach den Upgrades und Updates zu validieren und zu verifizieren? Schon diese beiden Fragestellungen zeigen, dass es gelingen muss, Softwarefunktionen sicher voneinander zu entkoppeln.

Praktikable Partitionierung ist gefragt

Nicht nur unter dem Aspekt der funktionalen Sicherheit ist diese Entkopplung gefragt. Sie vereinfacht auch die Workflows in der Entwicklung, wenn Software unterschiedlicher Hersteller auf ein und demselben Steuergerät betrieben wird. Zudem sorgt die Trennung dafür, dass Steuergeräte in Zeiten zunehmender Cyberkriminalität schwerer angreifbar sind. Hat sich ein Hacker Zugang zu einer Funktion verschafft,

stellt der Hypervisor eine weitere hohe Hürde für ihn dar. Eine wenig reizvolle Aussicht für die Cyberkriminellen, die ja einen größtmöglichen Schaden anrichten wollen.
Um die Entkopplung zu realisieren, sind verschiedene Ansätze denkbar. So könnte man Softwarefunktionen strikt auf jeweils eigene Steuerungshardware verteilen. Doch sowohl die Hardwarekosten als auch die Systemkomplexität sprechen dagegen. Realitätsnäher ist eine auf AUTOSAR basierende Architektur mit definierten Partitionierungs- und Separierungskonzepten.
Auf dieser Basis ist es möglich, Upgrades einzelner Funktionen zu realisieren und dabei die Beeinträchtigung weiterer Funktionen auszuschließen. So ist gewährleistet, dass die Modifikation einer Funktion keine umfassende Re-Validierung sämtlicher Software auf dem betreffenden Steuergerät erfordert. Um die AUTOSAR-Konzepte umzusetzen, sind jedoch Erweiterungen notwendig.

Lösungsansatz Hypervisor – aber wie?

Hier bietet sich der Einsatz eines Hypervisors an. Er partitioniert ein einzelnes Steuergerät in diverse virtuelle Maschinen (VM). Obwohl die Funktionen faktisch auf demselben Steuergerät laufen, wähnt sich die jeweilige Software in einem Zustand, in dem es für jede Funktion eine eigene Hardware gibt. Die Funktionen sind so strikt entkoppelt, dass sie ohne komplette Re-Validierung einzeln modifiziert werden können – und ihre verschiedenen Hersteller schon in der Entwicklung des Steuergeräts unabhängig von allen anderen arbeiten können. Softwarefehler oder böswillige Eindringlinge bleiben lokal auf eine einzelne virtuelle Maschine begrenzt.
Und es wird möglich, Software mit verschiedenen ASIL-Sicherheitseinstufungen (Automotive Safety Integrity Level) von der niedrigsten Stufe QM bis zur höchsten Anforderung ASIL D auf ein und demselben Steuergerät zu betreiben.
Bei allen Vorteilen kommt es bei einer Hypervisor-Lösung jedoch auf die Umsetzung an. Ohne Anpassung an das spezifische Umfeld im Fahrzeug droht Ungemach. So braucht ein Hypervisor üblicherweise ein eigenes Speichermanagement sowie einen sogenannten Hypervisor-Privilege-Modus, der die Zugriffsberechtigungen regelt. Dieser ist bei klassischen Ausführungen dreistufig: der Hypervisor selbst, die Basissoftware und die Applikationsfunktionen. Doch sowohl das entsprechende Speichermanagement als auch der dreistufige Privilege-Modus wird von heute eingesetzten Fahrzeug-Mikrocontrollern nicht unterstützt. Dies stand dem breiten Einsatz der Hypervisor-Technologie im Automobil bisher noch entgegen.
Bosch Automotive Electronics – Body Electronics (AE-BE) ist es in einem Projekt für einen großen OEM nun gelungen, die genannten Problemfelder mit dem ETAS Lightweight Hypervisor (ETAS RTA-LWHVR) zu entschärfen. Der optimierte Automotive-Hypervisor hat nur noch einen Speicherbedarf von 5 Kilobyte (kB) und die Zugriffszeiten konnten um Faktor vier bis fünf verbessert werden. Die neue Lösung ermöglicht, dass es zu keinerlei Beeinflussungen zwischen den virtuellen Maschinen kommt.
Im konkreten Projekt war ein zentrales Body-Steuergerät in elf virtuelle Maschinen partitioniert, die jeweils für Software von unterschiedlichen Zulieferern reserviert waren. Die ASIL-Einstufung reichte dabei von QM bis B.

Lightweight Hypervisor geht über AUTOSAR hinaus

Trotz der Menge und Heterogenität der Softwarefunktionen verlief deren per Lightweight Hypervisor gekapselter Betrieb völlig problemlos. Dies gelang, weil die virtuellen Maschinen zwar auf den gemeinsamen Speicher zugreifen, die Zugriffe und die Laufzeiten auf dem Kern aber klar geregelt sind.
Möglich wird die hohe Performance der Lösung durch Aufteilen der Rechnerkerne: einen Master Core und die Applikations-Cores. Während dem Master Core das Hardwaremanagement sowie der Betrieb der zentralisierten Basissoftware und einiger Software-Applikationen zukommt, beherbergen die Applikations-Cores die strikt getrennten virtuellen Maschinen (siehe Bild 1) – wahlweise mit aufgeteilten Laufzeitumgebungen (RTE) gemäß AUTOSAR oder auch mit nicht-AUTOSAR-konformer Software – und das auf ein und demselben Steuergerät.
Wichtig bei diesem Ansatz ist die entsprechende Inter-Core-Kommunikation (ICC). Sie wurde von Bosch AE-BE entwickelt. Funktionen können zusätzlich zur ohnehin garantierten Ausführungszeit weitere Zeitbudgets anfordern, ohne dass es zu Abstrichen bei der Ausführung anderer Funktionen kommt (siehe Bild 2). Die Echtzeitanforderungen sind also jederzeit gewährleistet.
Bei hohem Laufzeitbedarf, welcher die eigene Kapazität zu überlasten droht, können die virtuellen Maschinen beim Hypervisor anfragen, ob sie vorübergehend auf zusätzliche vorgehaltene Laufzeitfenster zugreifen können. In diesem Fall merkt der Hypervisor die virtuelle Maschine in einer Warteschleife vor. Ist ein Laufzeitfenster frei, erlaubt er der ersten virtuellen Maschine in der Schleife,

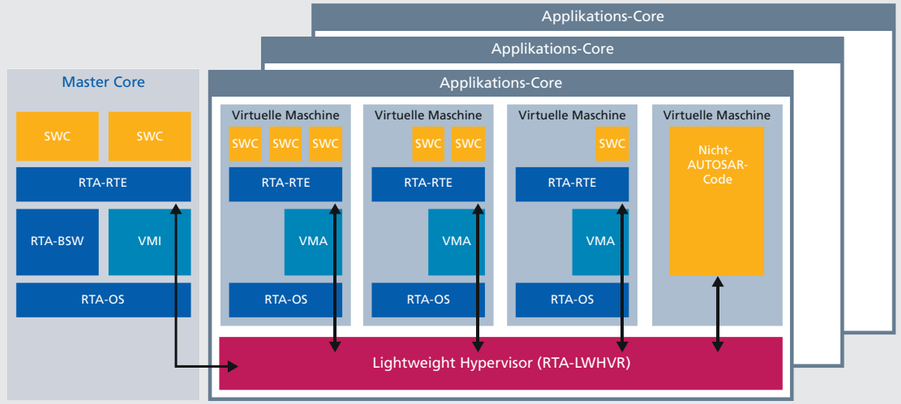


Bild 1:
Schematischer Aufbau eines Steuergeräts mit dem Lightweight Hypervisor RTA-LWHVR.

RTA-BSW AUTOSAR-Basissoftware
RTA-OS Betriebssystem
RTA-RTE Laufzeitumgebung
SWC Softwarekomponente in gesicherter Anwendung
VMA Adapter zur virtuellen Maschine
VMI Virtuelle Maschinenschnittstelle
ICC (Inter-Core-Kommunikation)
VM Virtuelle Maschine

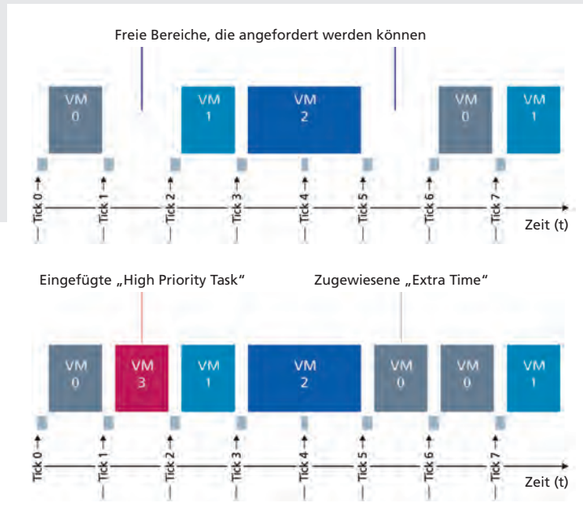


Bild 2: Zeitmanagement in einem Applikations-Core.

dieses zu nutzen. Durch dieses Vorgehen werden die Störungen durch eine hohe Systemlast minimiert. Jede virtuelle Maschine kann jedoch nur die Reservierung eines Fensters anfordern. So wird verhindert, dass eine fehlerhafte oder gehackte virtuelle Maschine die Kontrolle über das System erlangt.

Heute verfügbare, zukunftsfähige Lösung

Dank des gegenüber des klassischen Hypervisors drastisch reduzierten Overheads mit nur 5 kB Speicherbedarf und einem auf 5 Prozent der verfügbaren Kernkapazität reduzierten Leistungsbedarf, fügt sich der RTA-LWHVR problemlos in die spezifischen Randbedingungen für Embedded Systeme im Automobil ein. Er bietet volle Flexibilität für eine Vielzahl an Anwendungen und ist für zahlreiche Mikrocontroller verfügbar. Dabei gewährleistet er eine ebenso zuverlässige wie leistungsfähige Partitionierung von Steuergeräten, auf denen damit künftig Software unterschiedlicher Hersteller und Sicherheitsklassen betrieben werden können. Dank intelligenter Inter-Core-Kommunikation und strikter Kapselung können softwaregesteuerte Funktionen unabhängig voneinander entwickelt und – auch bei Fahrzeugen in Kundenhand – jederzeit ohne aufwendige Re-Validierung des Gesamtsystems modifiziert werden. Damit legt der Lightweight Hypervisor eine abgesicherte Basis für agile Software- und Funktionsentwicklung in der Automobilindustrie, die obendrein dynamische Security-Systeme mit regelmäßigen bedarfsgerechten Sicherheitsupdates möglich macht. Individuellen Konfigurationen und nachträglichen Upgrades von Fahrzeugen, wie bei Leon und seinen Eltern, steht damit nichts mehr im Wege.

Kontinuierliche Auslieferung von Steuergerätesoftware

Agile Software-Entwicklung beschleunigt die Elektrifizierung

Emissionsarme Fahrzeuge werden immer stärker nachgefragt. Um diesen Volumenmarkt zu bedienen, befinden sich bei allen OEMs neue Hybrid- und Elektromodelle in der Entwicklung. Die dafür erforderlichen Systeme – welche den Antriebsstrang effizient elektrifizieren – werden mit hoher Agilität entwickelt, um der hohen Frequenz an Kundenanforderungen entsprechen zu können. Die daraus resultierenden neuen Funktionen und Optimierungen der Steuergerätelogik werden im Produktbereich Leistungselektronik (GS-PE) der Robert Bosch Mobility Solutions kontinuierlich verbessert, getestet und freigegeben.

AUTOREN

M.Sc. Jochen Horinek ist Experte für Software-Tests im Produktbereich GS-PE der **Robert Bosch GmbH**.

Dipl.-Ing. Jörg Spranger ist Experte für Software-Entwicklung im Produktbereich GS-PE der **Robert Bosch GmbH**.

Zu diesem Zweck hat der Produktbereich Leistungselektronik die Entwicklung, die Integration und den Test von Funktionen für Inverter-Steuergeräte in einem hohen Grad automatisiert und parallelisiert. Basis hierfür ist die Toolumgebung „Application Lifecycle Management" (ALM), welche Entwicklern und Testern alle relevanten Informationen, wie Kundenanforderungen, gemeldete Fehler, Testfälle und Testreports, zur Verfügung stellt. Außerdem werden hier alle Arbeitsaufträge verfolgt, auf deren Basis die zuständigen Entwickler AUTOSAR-konforme Softwarekomponenten der jeweiligen Steuergerätefunktionen mithilfe von ETAS ASCET erstellen oder ändern.

Software wird kontinuierlich geprüft und freigegeben

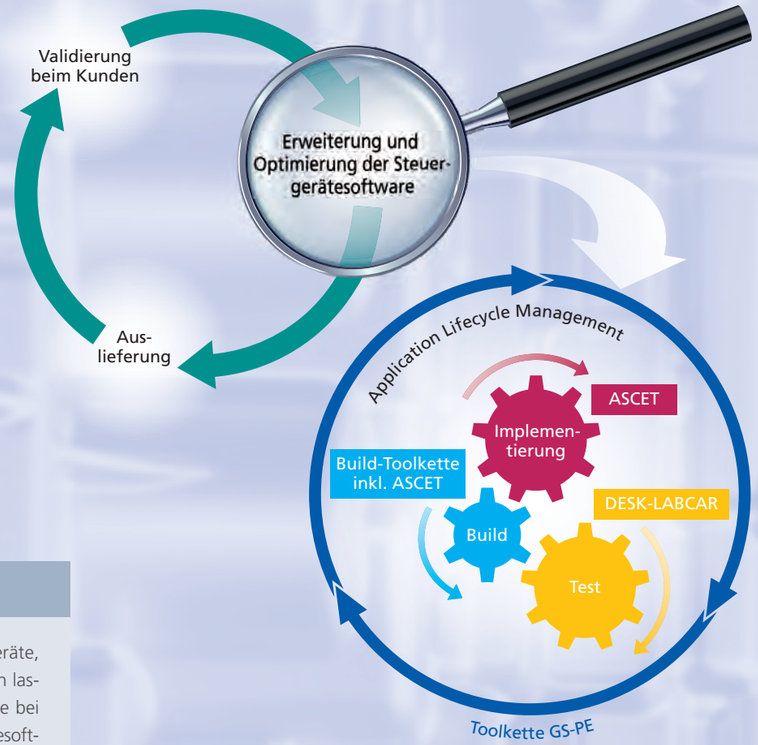
Nach der Entwicklung oder nach Änderungen bestehender Softwarekomponenten werden diese unmittelbar nach dem Einchecken in das System in die Steuergerätesoftware integriert sowie anschließend automatisch mittels statischer Code-Analyse in Bezug auf Codierfehler und Konformität zu Codierrichtlinien geprüft. Nach erfolgreicher Prüfung wird der neue Softwarestand mit ETAS INCA auf dem Steuergerät implementiert und konfiguriert. Anschließend wird das Steuergerät mithilfe von Echtzeit-Softwaresimulationen an einem ETAS DESK-LABCAR Closed-Loop-Tests unterzogen. Sind auch diese Tests mit Erfolg bestanden, ist der Softwarestand für weitere Validierungen an Hochvoltprüfständen freigegeben.

Vorteile

Bis auf die Tests neuer Funktionen kann der gesamte Ablauf von der Integration bis zur Report-Erstellung vollautomatisch erfolgen. In der Praxis stellen die Entwickler neue oder geänderte Softwarekomponenten am Abend in das System ein. Der Test kann dann über Nacht ablaufen. Auf Basis der Testergebnisse wissen die Entwickler bereits am nächsten Morgen, ob noch Korrekturen an bestimmten Komponenten vorgenommen werden müssen. Diejenigen Komponenten, für welche dies nicht der Fall ist, werden nach Abschluss des Testlaufs in einen neuen Softwarestand integriert. Dieser Softwarestand ist unmittelbar auf dem Steuergerät lauffähig und für weitere Prüfungen im Labor sowie später im Fahrzeug geeignet. Mithilfe der leistungsfähigen, miniaturisierten und kostengünstigen DESK-LABCAR-Systeme lassen sich die Hardware-in-the-Loop-Tests breit parallelisieren.

Kundennutzen

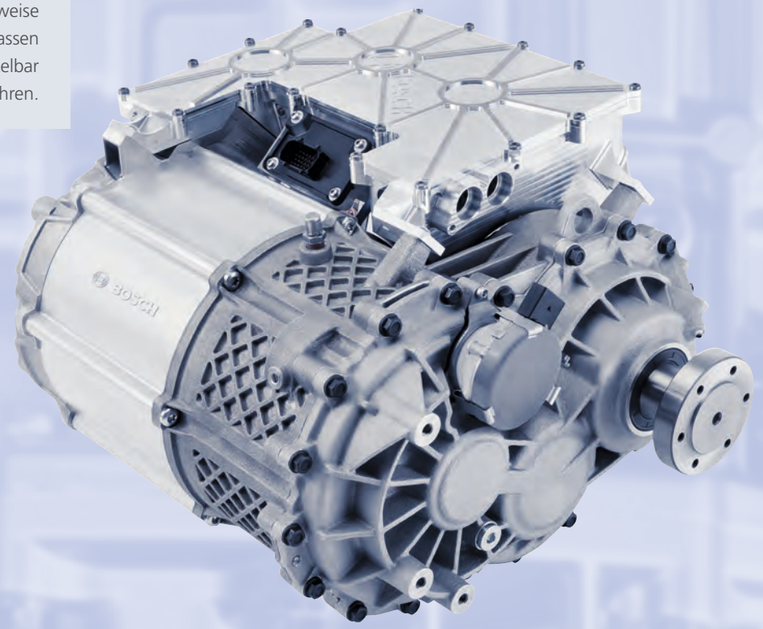
Die kontinuierliche Auslieferung von Software für Inverter-Steuergeräte unterstützt die agile, gemeinsame Entwicklung von Systemen des elektrischen Antriebsstrangs in hohem Maße. Die große Frequenz, mit der freigegebene Softwarestände für das Zielsystem zur Verfügung gestellt werden können, ermöglicht es, Lösungen in enger Abstimmung mit Kunden zu entwickeln und zu optimieren.



Die Toolkette des Produktbereichs GS-PE (rechts Mitte) ermöglicht die kontinuierliche Weiterentwicklung und Auslieferung von Software für Inverter-Steuergeräte (links oben). Die Toolkette ermöglicht es, Funktionen, die mit ASCET neu implementiert oder modifiziert werden, automatisch in die Software zu integrieren und zu testen. Der gesamte Ablauf wird durch ein Application-Lifecycle-Management-System unterstützt, in dem alle relevanten Daten verwaltet werden.

Ausblick

Durch den Einsatz virtueller AUTOSAR-Steuergeräte, die sich mithilfe von ETAS ISOLAR-EVE generieren lassen, können künftig zusätzliche Effizienzgewinne bei der kontinuierlichen Auslieferung von Steuergerätesoftware realisiert werden. Diese entstehen beispielweise beim Testen der Steuergerätesoftware. Hierbei lassen sich die Tests ohne Steuergerätehardware unmittelbar in der virtuellen Umgebung am Rechner durchführen.



Die neue eAchse von Bosch. Der Produktbereich GS-PE integriert Motor, Leistungselektronik und Getriebe. Hiermit kann eine Antriebsleistung zwischen 50 kW und 300 kW zur Verfügung gestellt werden. Die Software zur Steuerung des leichten und kompakten Achsantriebs wird von GS-PE mit ASCET und LABCAR entwickelt und getestet.

Neue Wege durch das Funktionslabyrinth

Eine Vielzahl an Werkzeugen hilft, schneller durch das Labyrinth der Funktionsentwicklung zu kommen. Jetzt gibt es noch eine andere Möglichkeit: die Softwarewerkzeuge SCODE-ANALYZER und SCODE-CONGRA von ETAS machen mit ihrer völlig neuen Methodik das Labyrinth einfacher! Erfahren Sie mehr über diese einzigartigen Tools.

AUTOR

Jürgen Crepin ist Senior Expert Marketingkommunikation bei der **ETAS GmbH**.

Methodik
Die Werkzeuge basieren auf dem Ansatz der funktionalen Morphologie, also dem Studium der Struktur und der Beziehungen der Funktionen untereinander, und der automatisierten Kognition, also dem Umgestalten von Informationen eines verhaltenssteuernden Systems.

Was bringen die Neuen?
Sie entlasten Entwickler von einfachen Routinearbeiten, wie der Analyse von Abhängigkeiten, dem Lösen von Gleichungen und der Generierung von Code für die nächsten Arbeitsschritte. Darüber hinaus unterstützen sie die Kreativität beim Finden der besten Lösung.

Anwendungsbereiche
System-, Funktions- und Softwareentwickler können von Beginn der Entwicklung an ihre komplexen Systeme beschreiben, visualisieren, analysieren und optimieren.

Simulink®-Anbindung
SCODE-ANALYZER und SCODE-CONGRA lassen sich einfach in MATLAB®/Simulink®-Umgebungen integrieren. Beide Werkzeuge erzeugen Code, der in MATLAB®/Simulink® weiterverarbeitet werden kann.

Enthusiasmus
Das Team, das in zehnjähriger Entwicklungsarbeit die prototypischen Werkzeuge aus der Forschung zur Serienreife gebracht hat, hatte sich viel vorgenommen. Ihr Anspruch: das Buch der Entwicklung von Embedded Software neu schreiben – wir glauben, sie haben es geschafft.

Schneller zum Ziel
Die ersten Projekte haben gezeigt, dass sich der Aufwand in der Funktionsentwicklung durch SCODE-ANALYZER und SCODE-CONGRA um teilweise mehr als **30 %** verringern lässt.

Nachweislich sicher
Die automatische Verifizierung der kompletten Beschreibung der Entscheidungspfade und mathematischen Beziehungen unterstützt die Anforderungen des Nachweises der funktionalen Sicherheit nach ISO 26262. Die Vollständigkeit der Betrachtung wird mathematisch bewiesen – das ist einzigartig.

Goethe, Zwicky und Michael Jackson?
Genau genommen beginnt die Geschichte von SCODE-ANALYZER und SCODE-CONGRA im 18. Jahrhundert. Johann Wolfgang von Goethe beschrieb mithilfe der Morphologie die Beziehungen der verschiedenen Lebensformen. Diese Grundidee inspirierte die Bosch-Forscher aus den Bereichen Mathematik, Computer- und Ingenieurwissenschaften und Philosophie. SCODE-ANALYZER und SCODE-CONGRA wurde von Ideen des Astronomen Fritz Zwicky, den Wissenschaftlern Stephen M. McMenamin und John F. Palmer und den britischen Computerwissenschaftlern Michael Jackson und George J. Friedman beeinflusst – erweitert um die Graphentheorie von Markus Behle, dem verantwortlichen Produktmanager.

Einfach „ein(e)clipsen"
Die neuen Werkzeuge können auf Basis von Eclipse einfach in bestehende Werkzeugketten integriert werden.

Sichere Verbindung
Der interdisziplinäre Ansatz der Tools verbindet die unterschiedlichen Paradigmen von klassischer IT-Entwicklung und regelungstechnischer Funktionsentwicklung.

Stets zu Diensten
ETAS bietet auch Consulting-Dienstleistungen, damit Kunden sich mit der neuen Methodik vertraut machen und die neuen Werkzeuge effizient nutzen können.

Neugierig geworden?
Mehr Informationen finden Sie unter www.etas.com/scode, www.etas.com/congra oder der Playlist „ETAS Expert Talk" auf unserem YouTube-Kanal.

SCODE-ANALYZER (System CO DEsign)

Das Werkzeug ermöglicht es, komplexe Zusammenhänge von Systemen jeglicher Art übersichtlich zu beschreiben und zu überprüfen. Dazu wird das Gesamtsystem in Betriebsbereiche, die sogenannten Modi, aufgeteilt. Das bringt vor allem Vorteile, wenn die Software viele Entscheidungen trifft oder viele Varianten hat. Das Ergebnis: massive Reduktion der Komplexität.

SCODE-CONGRA (CONstraint GRAphs)

Mit der SCODE-ANALYZER-Erweiterung SCODE-CONGRA kann der **Funktionsentwickler** das System exakt mathematisch und verständlich beschreiben und grafisch visualisieren. Regelverletzungen, Inkonsistenzen, algebraische Schleifen und andere relevante Eigenschaften des Systems werden präzise angezeigt. Der Anwender erhält sofort Optionen und Funktionen, um Fehler zu korrigieren. Auswirkungen von Veränderungen im System werden sehr verständlich dargestellt. Experimentieren durch Modifikation der einzelnen Bestandteile ermöglicht es, in kurzer Zeit verschiedene Variationen auszuprobieren und zu bewerten.
Der **Applikateur** erhält sehr gut vorkalibrierte Parameter sowie eine Darstellung der Sensibilität des Systems in relevanten Betriebspunkten. Dies ermöglicht ihm, sich zielgerichtet auf die wichtigen Teile des Systems zu konzentrieren und die vorkalibrierten Parameter im realen Betrieb zu optimieren.

Simulation und Virtualisierung von Fahrzeugsystemen

Entwicklung und Test verteilter Funktionen mit ETAS COSYM

Wie können Funktionen des automatisierten Fahrens, an denen zahlreiche elektronisch gesteuerte Systeme des Fahrzeugs beteiligt sind, innerhalb kurzer Zeit mit hoher Qualität und wettbewerbsfähigen Preisen zur Serienreife gebracht werden? Wie lassen sich komplexe Antriebe mit Elektro- und Verbrennungsmotoren, Fahrbatterie, Katalysatoren und Automatikgetriebe optimal auslegen?

AUTOREN

Dr. Ulrich Lauff ist Senior Expert Marketingkommunikation bei der **ETAS GmbH**.

Dr. Christoph Stoermer leitet den Bereich Vorausentwicklung bei der **ETAS GmbH**.

Deepa Vijayaraghavan ist als Produktmanagerin verantwortlich für das Werkzeug COSYM bei der **ETAS GmbH**.

Um neue Funktionen mithilfe von MiL-/SiL- und HiL-Umgebungen nahtlos entwickeln und flexibel testen zu können, werden leistungsfähige Umgebungen zur Generierung virtueller Steuergeräte, fortschrittliche Werkzeuge zur Integration und Konfiguration modular aufgebauter Systemmodelle und skalierbare Plattformen zur Ausführung von Simulationen benötigt.

ETAS COSYM

Mit COSYM lassen sich vernetzte Embedded Systeme in virtuellen Umgebungen effizient testen und validieren. COSYM bietet eine offene Simulationsplattform, die auf neuen Softwaretechnologien basiert (siehe Grafik). Im Kern ermöglicht COSYM durchgängige MiL-/SiL-/HiL-(XiL-)Tests von Systemen unter besonderer Berücksichtigung von Steuergerätenetzwerken.

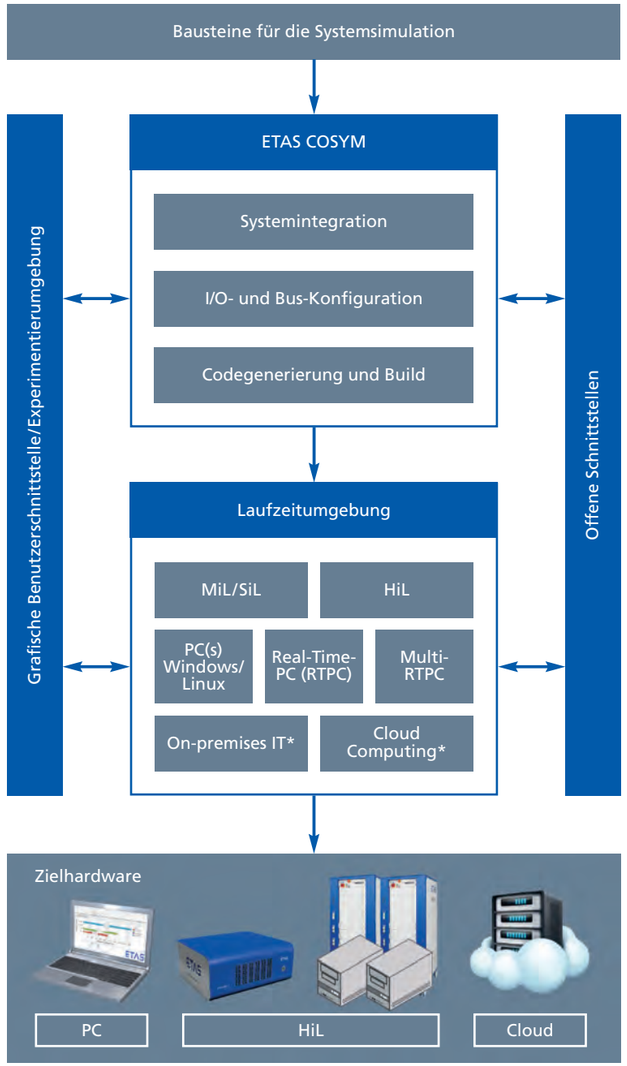
Gleichzeitig bietet COSYM eine Plattform für moderne „Continuous Integration"-Prozesse der System- und Software-Entwicklung. COSYM umfasst Werkzeuge für die folgenden Schritte:

- Erstellung eines Systemmodells, zum Beispiel durch Import von Strecken-, Funktions- und Restbusmodellen sowie deren Signalverknüpfung. Weiterhin werden die Erstellung virtueller Netzwerke und deren Verknüpfung mit virtuellen und physikalischen Steuergeräten ermöglicht. Das erstellte Systemmodell besteht somit nicht nur aus einer Signalkopplung von Modellen, sondern kann auch die Netzwerkkommunikation berücksichtigen. Wird das virtuelle Steuergerät auf der Ebene der Mikrocontroller-Abstraktionsebene eingebunden, zum Beispiel mit ETAS ISOLAR-EVE, kann eine deutlich genauere Simulation erfolgen als im Vergleich zu einer Einbindung auf Applikationssoftware-Ebene.
- Konfiguration der Simulation für MiL-, SiL- und HiL-Umgebungen, abhängig von der Ausführungsplattform und dem Zeitverhalten (Echtzeit oder synchron zur Zeitskala der Simulation).
- Durchführung von Experimenten mithilfe der bewährten ETAS-Experimentierumgebung.
- Automatisierung über die XiL-API oder die native REST-Schnittstelle, welche eine moderne softwaretechnische Anbindung von „Continuous Integration"-Umgebungen ermöglicht. Damit erlaubt COSYM die Projekterstellung und zukünftig auch das Experimentieren im Serverbetrieb.

COSYM basiert auf einer modernen Softwaretechnologie mit konsequenter Trennung von Services und Benutzerführung. Die gut dokumentierte REST-Schnittstelle zu den Services ermöglicht eine einfache Integration in eigene Benutzerführungen oder Automatisierungen. COSYM beinhaltet standardmäßig eine webbasierte Benutzerschnittstelle. Durch die serviceorientierte Architektur kann die Plattform aber auch in integrierte Entwicklungsumgebungen (IDEs) wie Eclipse eingebunden werden.

Markteinführung

Die Einführung von COSYM wird in drei Phasen im Rahmen von Pilotprojekten erfolgen. Ab Ende 2017 steht COSYM für ETAS-LABCAR-HiL-Systeme zur Verfügung. Dadurch wird die Vorverlagerung von HiL-Tests in rein virtuelle Umgebungen zum Beispiel auf dem PC ermöglicht. Hierfür können unter anderem Streckensimulationen der LABCAR-MODEL-Familie verwendet werden. Werden die physikalischen Steuergeräte durch virtuelle Steuergeräte oder geeignete Funktionsmodelle ersetzt, ist die Virtualisierung des Gesamtsystems möglich.



* in Zukunft möglich

In der zweiten Phase können bis Mitte 2018 virtuelle Netzwerke für alle gängigen Fahrzeugbusse integriert werden. Zusätzlich dazu werden virtuelle Zeitskalen als Alternative zur Echtzeitsimulation sowohl von COSYM als auch von LABCAR-MODEL unterstützt. Damit lassen sich Tests wesentlich schneller als in Echtzeit am HiL durchführen.

In Phase Drei, ab Mitte 2018, werden die Voraussetzungen für die Kalibrierung komplexer Systeme in virtuellen Umgebungen geschaffen. Das besondere Augenmerk liegt dabei einerseits auf der Emissionierung von Antrieben im Hinblick auf den tatsächlichen Fahrbetrieb (Real Driving Emissions, RDE). Andererseits lassen sich so in Zukunft ADAS- und Fahrautomatisierungs-Anwendungen, beispielsweise mithilfe von Messdaten aus Fahrversuchen, in der virtuellen Umgebung anpassen und trainieren.

ETAS COSYM – Systemübersicht.

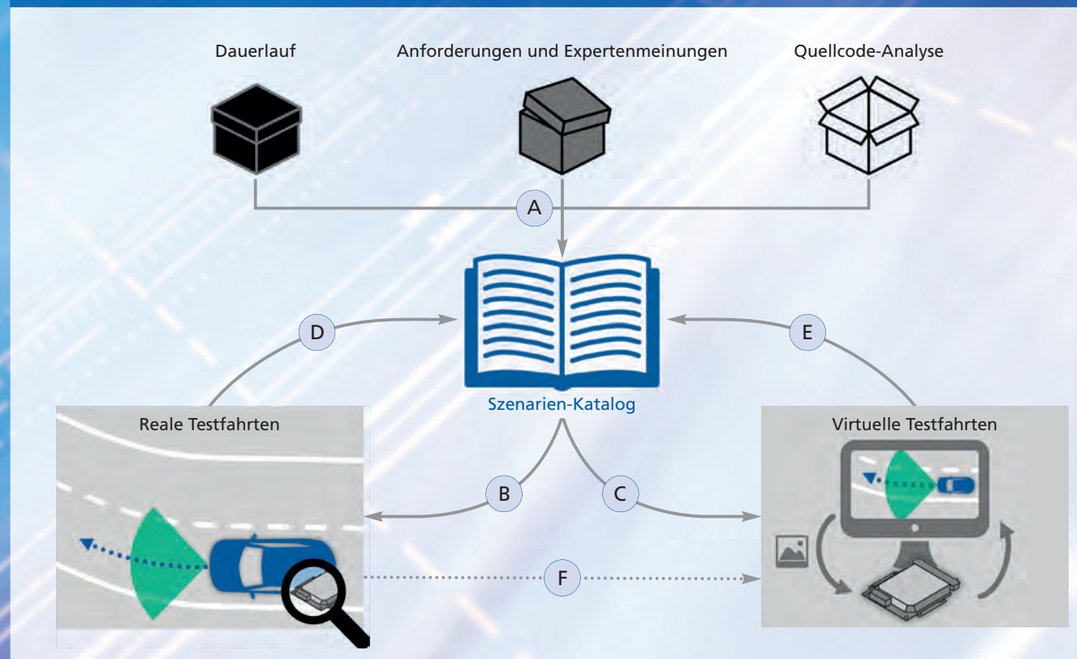
Ausblick

Die COSYM-Plattform wird mittelfristig für die Ausführung auf leistungsfähigen Serverinfrastrukturen, wahlweise im Unternehmen (on-premises) oder in einer externen Cloud ausgebaut. Um die datenintensive Entwicklung von Systemen für das autonome Fahren noch besser zu unterstützen, wird ein weiterer Schwerpunkt in der Anbindung von Big-Data-Lösungen liegen, mit denen in großen Datenbeständen schnell auf geeignete Messdaten für den Vergleich oder die Kombination mit Simulationen zugegriffen werden kann.

Robuste Assistenzsysteme

Iterative Absicherungsstrategie

Wie lassen sich softwaregesteuerte Assistenzsysteme für autonome Fahrzeuge effizient absichern? Da sich Verkehrsgeschehen und Umweltbedingungen vorab kaum vollständig in Systemspezifikationen erfassen lassen, sind robuste Softwaresysteme gefragt. Der Weg dahin führt über virtualisierte Tests auf Basis iterativ erweiterbarer Szenarien-Kataloge.



Schematische Darstellung des Absicherungsansatzes. A–F = Vorgehensweisen (siehe Text).

Womit werden Passagiere autonomer Fahrzeuge ihre neu gewonnene Zeit verbringen? Ob mit Büroarbeit, Onlineshopping oder Wellness bleibt dem Fahrgast überlassen. Klar ist aber, dass Autofahrer nur dann die Hand vom Lenkrad nehmen werden, wenn sie der Technik hundertprozentig vertrauen.

Es wird nicht mehr genügen, aktive Assistenzsysteme gemäß ISO 26262 auf den Fall eines Systemversagens auf funktionaler Ebene vorzubereiten. Sie müssen für das automatisierte Fahren auch gegen situative Fehlinterpretation abgesichert werden. Der Haken: Verkehrsszenarien, Wetter- und Lichtverhältnisse sind zu heterogen, um vorab alle Eventualitäten in Systemspezifikationen erfassen zu können. In der Softwarewelt hat diese Problematik einen Namen: funktionale Unzulänglichkeit.

Die Antwort darauf heißt Robustheit. Robuste Software muss auch in ungewöhnlichen Situationen definiert arbeiten und sinnvolle Reaktionen auslösen. Übertragen auf das autonome Fahren liefe das darauf hinaus, die Robustheit der softwaregesteuerten Assistenzsysteme trotz der zwangsläufig unvollständigen Spezifikationen auf ein gesellschaftlich akzeptables Niveau zu bringen – also bei allem Pragmatismus stets das höchstmögliche Sicherheitsniveau anzustreben.

Äquivalenzklassenbasierte Szenariobeschreibung

Aktuelle Fachaufsätze zeigen das Ausmaß dieser Aufgabe. So führt etwa der Darmstädter Professor Hermann Winner an einem wahrscheinlichkeitsbasierten Absicherungsansatz für einen Autobahnautomaten vor, dass schon für diese vergleichsweise einfache Anwendung **2,4 • 10^8 Kilometer** Fahrstrecke nötig wären, um nachzuweisen, dass Fahrzeuge mit diesem System auf Autobahnen maximal halb so viele Unfälle mit Personenschäden verursachen wie Fahrzeuge ohne den Autobahnautomaten.

Zur Absicherung gilt es zu klären, mit welcher Wahrscheinlichkeit **P** ein System eine Metrik **M** erfüllt. Aufgrund des Einsatzortes d_E **= Autobahn** ist diese Wahrscheinlichkeit bedingt durch: **P(M|Autobahn)**.

Soll das Systemverhalten abseits der Autobahn mitbetrachtet werden, ist der Einsatzort d_E **= Nicht-Autobahn**. Die Gesamtwahrscheinlichkeit zur Erfüllung der Metrik wird dadurch zu P_{ges}**(M) = P(M|Autobahn) • P(Autobahn) + P(M|Nicht-Autobahn) • P(Nicht-Autobahn)**.

In Testfahrten könnte sich herausstellen, dass der Einsatzbereich Nicht-Autobahn in die zwei unterschiedlichen Teile „innerorts“ und „außerorts“ aufgeteilt werden muss.

Verhält sich das zu testende System jeweils innerhalb eines klassifizierten Bereichs äquivalent, so lässt sich die Dimension Einsatzort in drei Äquivalenzklassen aufteilen: d_E **= {Autobahn, innerorts, außerorts}**.

Im Zuge einer Testkampagne könnte sich ergeben, dass das System auf trockener Straße einwandfrei arbeitet, auf nasser Straße aber häufig versagt. Dies ließe sich dann durch die Einführung einer weiteren Dimension Straßenbeschaffenheit d_S **= {trocken, nass}** in die Beschreibung aufnehmen. Damit wären bereits sechs Szenarien in der Metrik zu prüfen.

Allgemein lässt sich ein Szenario **S** als die Kombination je einer Äquivalenzklasse jeder Dimension definieren $S = [d_1, d_2, \ldots d_n]$. Die Gesamtwahrscheinlichkeit zur Erfüllung der Metrik ergibt sich allgemein für n Dimensionen d_n zu

$P_{ges}(M) = \sum P(M|S_i) \cdot P(S_i)$,

wobei sich die Anzahl an Szenarien i aus der Mächtigkeit an Äquivalenzklassen aller Dimensionen zu $i = \prod |d_n|$ ergibt. Die Bestimmung $P(M|S_i)$ bedarf im Experiment konkreter Testfälle, die jeweils ein Szenario repräsentieren. Die Gesamtsumme verschiedener Szenarien dient als Referenzgröße der Anzahl unterschiedlicher Testfälle und ist für die belastbare Absicherung des Systems essentiell.

Iterative Erweiterung der Szenario-Beschreibung

Diese Äquivalenzklassen-motivierte, iterativ verfeinerte Szenario-Beschreibung kann nun in einem anwendungsorientierten Prozess zur Absicherung autonomer Systeme angewandt werden, der in der Grafik links visualisiert ist.

Im Zentrum der iterativen Absicherungsstrategie steht ein Szenarien-Katalog, der sich aus drei Quellen (A) speist: Ereignisse aus Dauerläufen und Felderprobungen, bei denen das System nicht wie erwartet reagiert hat. Konstruierte Szenarien auf Basis von Systemspezifikationen und Experteneinschätzungen. Und weitere, aus statischen Quellcode-Analysen generierte Szenarien.

Dieser Szenarien-Katalog dient sowohl der Systematisierung realer Testfahrten (B) als auch zur Parametrierung virtueller Testfahrten (C). Letztere haben den Vorteil, dass sie von der Verfügbarkeit teurer Versuchsfahrzeuge entkoppelt und auf beliebig vielen Rechnern parallel durchführbar sind. Auch lassen sich kritische Situationen, die bei Testfahrten auftreten, nach Bedarf reproduzieren und abwandeln. Aus diesen Variationen können Entwickler neue Szenarien herleiten, diese analysieren und sie in den Katalog einfließen lassen (D, E). So ist die kontinuierliche Verbesserung der Testabdeckung gewährleistet. Zur Absicherung der domänenübergreifenden Gesamtsimulation von Assistenzsystemen ist es erforderlich, die einfließenden Modelle (F) im Abgleich realer und virtueller Fahrversuche zu validieren. Erst der Vergleich erlaubt verlässliche Aussagen zur Genauigkeit der Gesamtsimulation und zu den Gültigkeitsbereichen der Modelle. Zudem führt er nach und nach zu einer immer exakteren, umfassenderen Grundlage für die virtuelle Erprobung von Assistenzsystemen. Virtualisierung wird dadurch zum Schlüssel für steigende Qualität bei zugleich sinkendem Kosten-, Zeit- und Organisationsaufwand.

AUTOREN

Marius Feilhauer betreut die Entwicklung von Simulationsmodellen für Fahrerassistenzsysteme im Bereich Test und Validierung bei der **ETAS GmbH**.

Dr. Jürgen Häring ist Leiter des Produktmanagements im Bereich Test und Validierung bei der **ETAS GmbH**.

ETAS INCA-RDE

AUTOREN

Dr. Ulrich Lauff ist Senior Expert Marketingkommunikation bei der **ETAS GmbH**.

Rajesh Reddy ist als Produktmanager verantwortlich für das Werkzeug INCA-RDE bei der **ETAS GmbH**.

Bestimmung von Emissionen im tatsächlichen Fahrbetrieb

Im Rahmen von Fahrzeugzulassungen in Ländern der EU müssen ab 2017 die Schadstoffemissionen im tatsächlichen Fahrbetrieb (Real Driving Emissions, RDE) überprüft werden. Zur Überwachung der Konformität von RDE-Messungen mit den gesetzlichen Vorgaben hat ETAS einen Assistenten entwickelt, der den Testfahrer in Echtzeit über den Status der Messung informiert. Damit RDE-Tests in der gewohnten Arbeitsumgebung durchgeführt werden können, wurde der Assistent nahtlos in ETAS INCA integriert. Mit der Lösung lassen sich RDE-Testfahrten kontrolliert und reproduzierbar durchführen.

Bei RDE-Messungen muss eine Vielzahl von Parametern beachtet und berücksichtigt werden. Diese betreffen beispielsweise die Dauer der Messfahrt, die Streckenlängen, die innerorts, außerorts und auf der Autobahn gefahren werden müssen, zulässige Geschwindigkeitsintervalle und Anforderungen an die Fahrdynamik. Gleichzeitig benötigen die Versuchs- und Applikationsingenieure die aktuellen Ergebnisse der Emissionsmessungen.

ETAS INCA-RDE

Der RDE-Assistent, der von ETAS als Produkt mit der Bezeichnung INCA-RDE angeboten wird, wertet die Messdaten während der Versuchsfahrt in Echtzeit aus (siehe Bild 1). Mithilfe von RDE-spezifischen, virtuellen Instrumenten werden dem Testfahrer im INCA-Experiment folgende Informationen von INCA-RDE angezeigt:

- GPS-Positionsdaten
- Start der Emissionsmessungen
- Messergebnisse
- Messeinrichtungsüberwachung

Zusätzlich dazu werden die folgenden Versuchsparameter angezeigt:

- Umgebungsbedingungen und Motorzustand
- Streckenlänge und Fahrtzeit je Streckenkategorie
- Fahrzeuggeschwindigkeit und Beschleunigung
- Abschätzung der Konformität der Messfahrt mit den RDE-Anforderungen

Auf Bild 2 ist exemplarisch der Screenshot eines virtuellen Instruments dargestellt, mit dem RDE-Daten im INCA-Experiment angezeigt werden.

Funktionsweise

Das Softwarewerkzeug INCA-RDE wird über CAN mithilfe eines ES59x-Schnittstellenmoduls mit der PEMS-Hardware (Portable Emissions Measurement System) verbunden. Zusammen mit OBD- und GPS-Daten, die das PEMS ebenfalls erfasst, werden die gemessenen Emissionen mit INCA-RDE online ausgewertet. Dabei werden die Fahrdynamikbedingungen von INCA-RDE sowohl mit der Methode der gleitenden Mittelung (EMROAD) als auch durch das Verfahren der Einstufung in Leistungsklassen (CLEAR) überprüft. Die Analyse-Ergebnisse, die eigentlichen RDE-Daten, werden zum einen im INCA-Experiment in den RDE-spezifischen Instrumenten angezeigt und zum anderen zeitsynchron zu Signalen aus dem Motorsteuergerät von INCA im 10-ms-Takt aufgezeichnet. Die erfassten RDE-Daten lassen sich deshalb im Anschluss an die Messung einfach mit Messsignalen aus der Motorsteuerung korrelieren.

Fazit

INCA-RDE stellt Versuchsingenieuren Informationen über die Ausführung und Auswertung von RDE-Messungen während der Testfahrt mithilfe von übersichtlichen Anzeigeinstrumenten in Echtzeit zur Verfügung. Mithilfe der Lösung, die in die vertraute Werkzeugumgebung für Messungen im Fahrzeug, Steuergerätekalibrierung und Diagnose integriert ist, lassen sich RDE-Messungen effizient durchführen und mit Signalen aus der Motorsteuerung korrelieren.

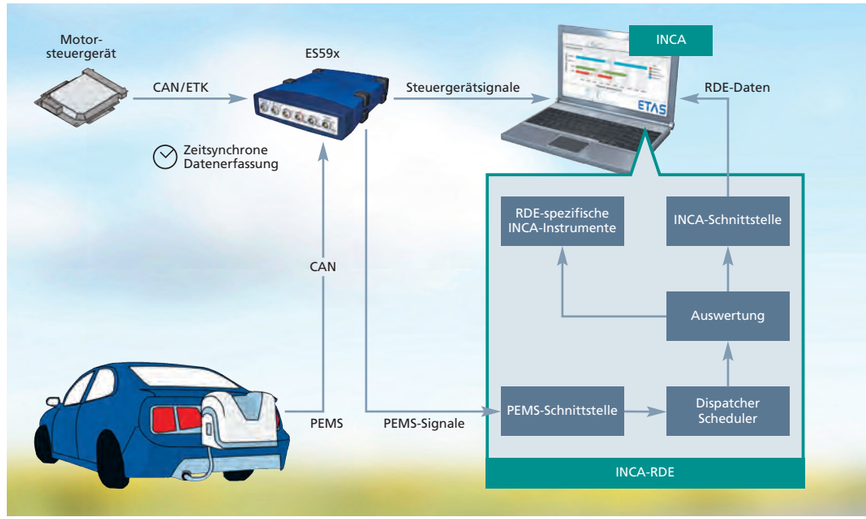


Bild 1: Systemübersicht INCA-RDE. Die Emissionen werden mit einer transportablen Messeinrichtung (PEMS) im Fahrversuch gemessen, mit INCA-RDE ausgewertet und in INCA mithilfe von spezifischen Instrumenten angezeigt.

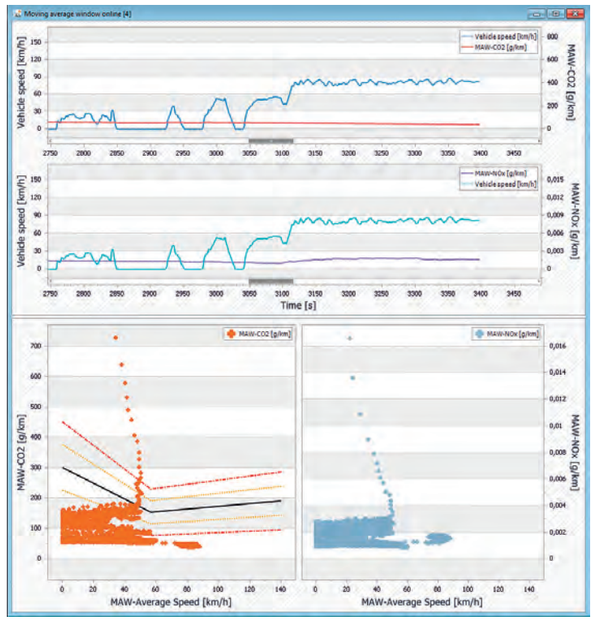
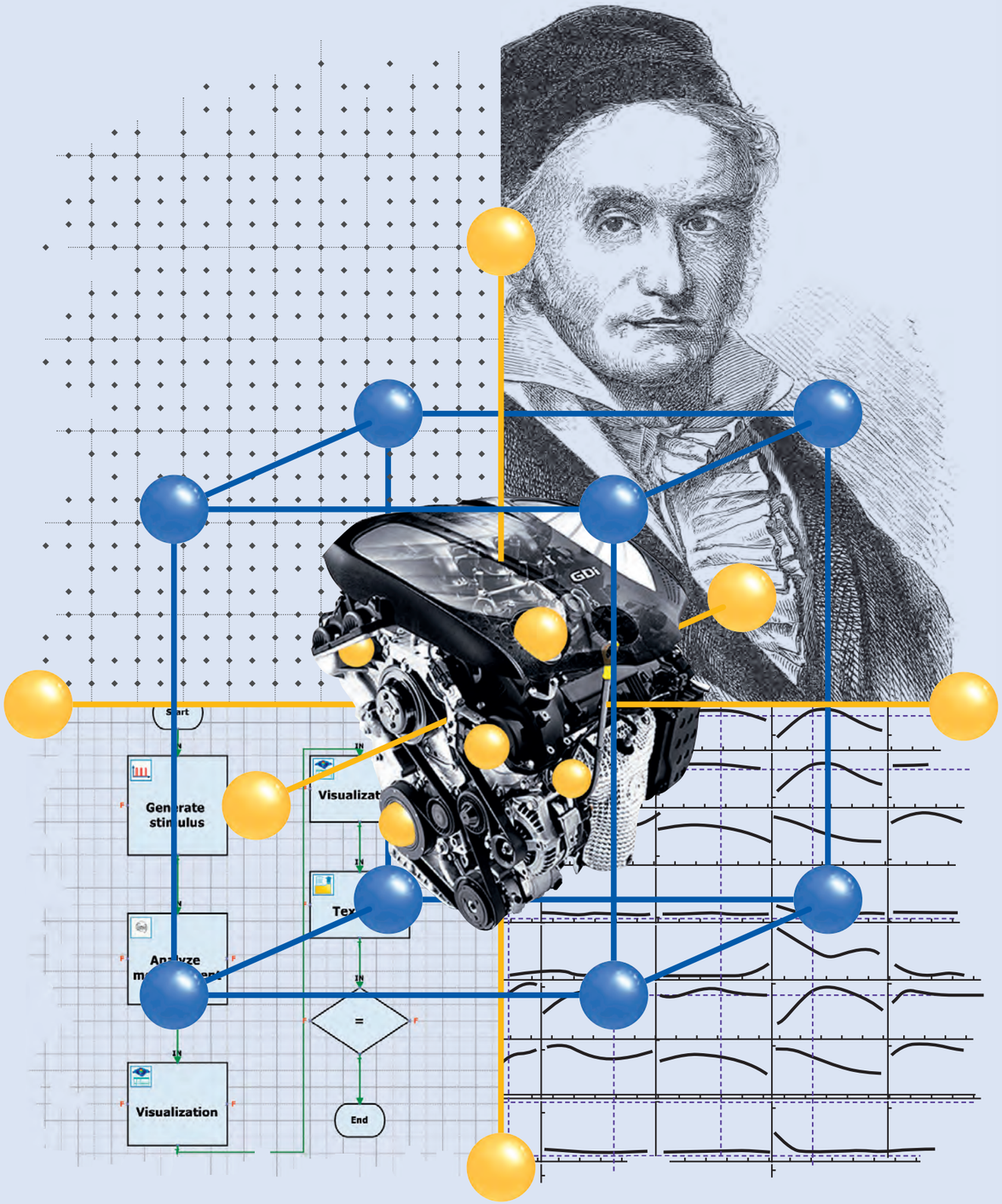


Bild 2: Oben und in der Mitte – CO_2- und NO_X-Emissionswerte in g/km und Fahrzeuggeschwindigkeit gegen die Messzeit in Sekunden. Unten – CO_2- und NO_X-Emissionen gegen die Fahrzeuggeschwindigkeit. Im Diagramm unten links sind die charakteristische CO_2-Kurve (schwarze Linie) des Versuchsfahrzeugs und die dazugehörigen Toleranzbänder (gelbe und rote Linien) eingezeichnet. Bei der RDE-Prüfung soll die Hälfte der CO_2-Werte, die innerhalb eines Fensters mit variabler Breite (Moving Average Window, MAW) gemittelt werden, innerhalb des inneren Toleranzbands liegen.



Optimierung von Ottomotoren

AUTOREN

Yooshin Cho ist leitender Ingenieur im Bereich Methodik von Ottomotorentests im **Hyundai R&D Center**, Namyang, Korea.

Wonseok Chang und **Wongeun Yoo** sind Field Application Engineers bei **ETAS Korea Co., Ltd**.

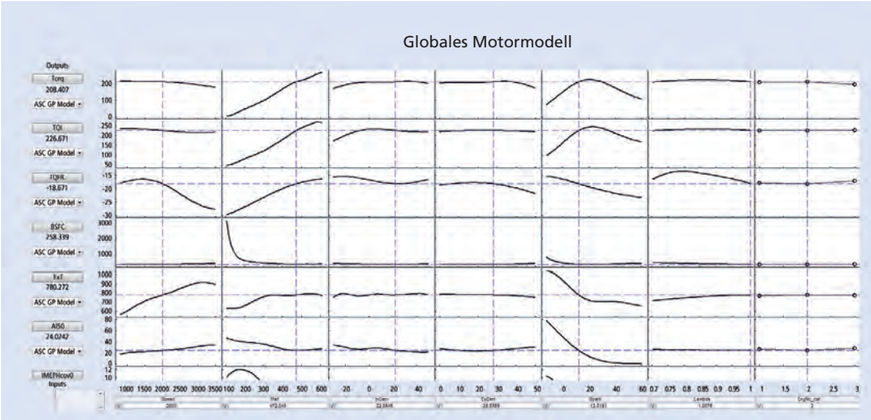
Modellbasierte Applikation bei Hyundai

Um den hohen Anforderungen in Bezug auf Leistung, Kraftstoffverbrauch und Schadstoffemissionen zu entsprechen, werden immer effizientere Motoren entwickelt. Die große Anzahl von Freiheitsgraden, die mit der Menge an Systemen einhergeht, spiegelt sich in einer Vielzahl von Parametern wider, die im Zuge der Applikation angepasst und optimiert werden müssen.

Die Hyundai Motor Company (HMC) führte in ihrem Forschungs- und Entwicklungszentrum in Namyang in Südkorea aus diesem Grund einen neuen, modellbasierten Applikationsprozess ein, der zum einen effizient ist und zum anderen den Betriebsbereich des Motors global abdeckt. Der neue Prozess fußt auf fortschrittlichen Modellierungs- und Automatisierungsmethoden, welche von den Softwaretools ETAS ASCMO und ETAS INCA-FLOW unterstützt werden.

Aufgabenstellung

Die Einsparung des Messaufwands im Vergleich zum bisherigen Prozess und die Qualität der Ergebnisse wurden von Hyundai anhand üblicher Applikationspakete für Ottomotoren bestimmt. Gegenstand der Untersuchungen war ein direkteinspritzender 3-Liter-V6-Saugmotor mit dreistufigem Ansaugsystem, doppelter, kontinuierlich verstellbarer Ventilsteuerung und einem Motorsteuergerät von Continental. Dafür wurden die Steuerzeiten von Ein- und Auslassnockenwelle, die Einspritzzeiten und der Zündwinkel optimiert sowie die Modelle für die Füllung, das Moment und die Abgastemperatur im Steuergerät bedatet.



Torq (Nm) = Drehmoment (Nm)
BSFC (g/kWh) = Spezifischer Kraftstoffverbrauch (g/kWh)
ExT (°C) = Abgastemperatur (°C)
IMEPHcov0 (%) = Variationskoeffizient des effektiven Mitteldrucks im Brennraum (%)

Bild 1: Grafische Darstellung der Abhängigkeiten der Ausgangs- von den Eingangsgrößen; das ETAS-ASCMO-Modell gibt die Abhängigkeiten im gesamten Parameterraum sehr gut wieder.

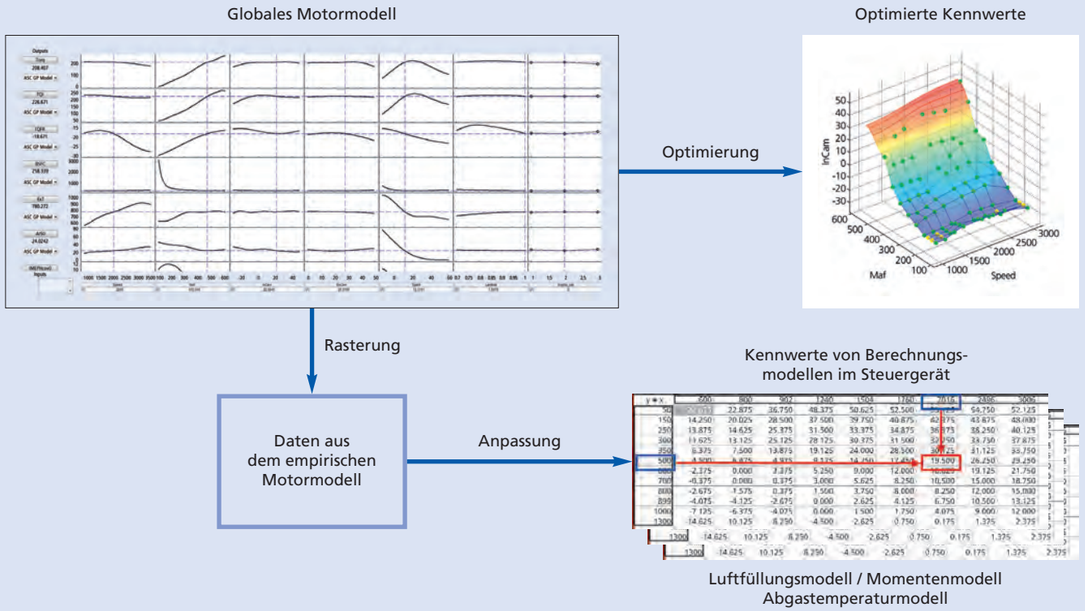


Bild 2: Optimierung der Parameterwerte von Modellen im Steuergerät durch Anpassung der Ausgaben dieser Modelle an Daten, die mit ETAS ASCMO aus dem empirischen Motormodell abgerastert werden.

Neuer Applikationsprozess

Mit der Umgestaltung des Applikationsprozesses hat Hyundai zwei neue Methoden eingeführt, nämlich die statistische Versuchsplanung (Design of Experiments, DoE) sowie die vollautomatisierte Vermessung des Motors am Prüfstand. Mit maschinellen Lernverfahren werden Modelle, die das Verhalten von Motoren mit hoher Genauigkeit am Computer nachbilden, auf Basis der Messergebnisse generiert. Die Versuchspläne und die messdatenbasierten Modelle werden mit dem Werkzeug ETAS ASCMO erzeugt. Die Messpunkte der Versuchspläne lassen sich am Prüfstand mithilfe einer auf Basis des Werkzeugs INCA-FLOW neu entwickelten Messsteuerung vollautomatisch abfahren.

Applikation auf Basis des Motormodells

Das aus den Messungen am Prüfstand erstellte Motormodell gibt das Verhalten des Motors im gesamten Parameterraum mit hoher Genauigkeit wieder (siehe Bild 1). Auf Basis des Modells wurden sowohl der Kraftstoffverbrauch als auch das Volllastdrehmoment optimiert (siehe Bild 2). Die Klopfgrenze und die Obergrenze für die Abgastemperatur wurden dabei eingehalten. Die Bedatung des Füllungs-, Momenten- und Abgastemperaturmodells im Steuergerät erfordert große Mengen an Daten. Diese wurden nicht, wie beim konventionellen Vorgehen üblich, aufwendig am Motorenprüfstand gemessen, sondern von ETAS ASCMO aus dem empirischen Motormodell abgeleitet. Beim Vergleich mit Validierungsmessungen betrugen die Abweichungen der Ergebnisse, die mit den so bedateten Modellen berechnet wurden, beim Füllungsmodell weniger als 5 %, beim Momentenmodell weniger als 5 % oder maximal 5 Nm und beim Abgastemperaturmodell weniger als 15 °C.

Fazit

Durch die Einführung des globalen, modellbasierten Prozesses im Forschungs- und Entwicklungszentrum in Namyang konnte Hyundai eine drastische Effizienzsteigerung bei der Applikation von Motoren erreichen. Mit dem neuen Prozess ließ sich der Messaufwand am Motorenprüfstand im Vergleich zur konventionellen Vorgehensweise um 75 % verringern. Gleichzeitig wurden die zu Beginn definierten Projektziele erreicht.

Zusammenfassend kann gesagt werden, dass der globale, modellbasierte Prozess eine effiziente Applikation komplexer Motoren mit hoher Qualität ermöglicht.

ASCET im Hochschullabor

Modellbasierte Software-Entwicklung an der Universität Stuttgart

Im Rahmen einer Kooperation mit der Universität Stuttgart leiten die ETAS Resident Engineers Andy Staats und Christoph Schlegel das Unipraktikum „Modellbasierte Entwicklung automobiler Software“. Die Studierenden lernen bei dieser Lehrveranstaltung die Software-Architekturen und die Vorgehensweisen bei der Programmierung von Steuergeräten kennen. Hierbei bildet insbesondere die modellbasierte Entwicklung eingebetteter Automobilsoftware einen Schwerpunkt. Der wichtigste Part der Veranstaltung: die praktischen Laborübungen. Hier kommen Methoden der Steuergerätesoftware-Entwicklung zur Anwendung. Dabei modellieren die Studierenden Steuergerätefunktionen in ETAS ASCET und testen diese mit Rapid-Prototyping-Systemen wie dem Prototyping- und Schnittstellenmodul ES910 von ETAS. „In unserem ASCET-Labor profitieren die Studierenden davon, dass sie in kleinen Gruppen viele Übungen machen, dabei ihr erlerntes Wissen anwenden und so aus möglicherweise gemachten Fehlern direkt lernen können“, so Andy Staats. Dabei betont er: „Der größte Vorteil für die Studierenden ist, dass sie Vorgehensweisen sowie Soft- und Hardware kennenlernen, die tatsächlich in der Industrie eingesetzt werden.“ Theorie und Praxis in Kooperation – eine gewinnbringende Kombination.

Im ASCET-Labor an der Universität Stuttgart lernen Studierende Software-Entwicklung hautnah unter Anwendung von praxiserprobten Methoden und Tools kennen.

Studierende entwickeln autonome Rennfahrzeuge

Mit ETAS zukünftige Technologien praktisch erlernen

Die Formula Student Germany ist nichts anderes als ein Spiegelbild der Entwicklung in der Automobilindustrie. Dazu gehört neben des Know-hows von Verbrennungs- und Elektromotoren auch der Wissensaufbau rund um das Thema autonomes Fahren. Daher gibt es seit diesem Jahr die Formula Student Driverless (FSD), bei der interdisziplinäre Zusammenarbeit immens wichtig ist. Neben Studierenden der Fachrichtungen Fahrzeugtechnik und Elektrotechnik sind vor allem Studierende der Informatik, Datenverarbeitung und Sensorik gefragt, um am Ende ein Rennfahrzeug zu entwickeln, das dem Regelwerk der FSD genügt.

Als langjähriger Sponsor von Formula-Student-Teams unterstützt ETAS seit 2017 auch die FSD. Dabei profitieren die Teams neben finanziellen Mitteln und technischem Support von ETAS-Experten vor allem vom gesamten ETAS-Produktportfolio. Somit bauen die Studierenden nicht nur ihr fachliches Wissen weiter aus, sondern setzen bereits jetzt ETAS-Produkte ein, um ganz vorne in der Rennserie mit dabei zu sein.

KA-RaceIng Driverless 2017 (Karlsruher Institut für Technologie).

Faszination ETAS-Messtechnik!

Auszubildende bauen Messfahrzeug für Studierende

Das ETAS Demo Car entstand aus der grundlegenden Frage der Schwieberdinger Ausbildungsabteilung von Bosch an ETAS: Wie kann man Messtechnik für Studierende erlebbar machen?

AUTOR

Klaus Fronius ist Hochschulbetreuer bei der **ETAS GmbH**.

Das ETAS Demo Car zog auf der embedded world 2017 viele Blicke auf sich.

Die Wandlung vom serienmäßigen Plug-in-Hybrid zum Blickfang mit Hightech-Innenleben war nach einigen Monaten perfekt. Eine breite Palette an ETAS-Messmodulen (ES4xx, ES5xx, ES6xx, ES9xx sowie die neue ES8xx-Serie) finden im neu gestalteten Interieur Platz. Aber was bringt die viele Hardware, ohne die entsprechende Software? Daher wurde in der ersten Ausbaustufe ETAS INCA-TOUCH in das Fahrzeug integriert. Dieses ist über den fest eingebauten Touchmonitor bedienbar. Obendrein lassen sich die Funktionen in INCA per Sprachbefehl ansteuern.

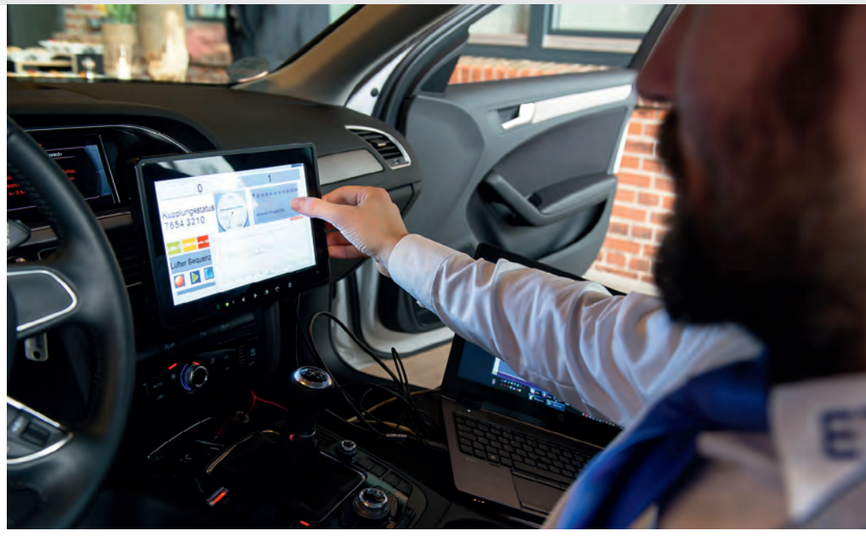
Was als praktisches Ausbildungskapitel für die Techniker und Auszubildenden begann, ging nahtlos in Phase Zwei der Wandlung über: Auf Messen und Innovationstagen in ganz Europa hat das schicke ETAS Demo Car in den letzten Monaten jede Menge Aufmerksamkeit auf sich gezogen. Ob in Frankreich, Belgien, Italien, England oder auf der embedded world 2017 in Nürnberg – das Interesse für das Demo Car war groß. Der Umbau macht Messtechnik direkt am Objekt erlebbar und demonstriert anschaulich, dass die Zeiten von Kabelgewirr und lose mitgeführten Laptops in Messfahrzeugen zu Ende gehen.

Die Auslandstournee war nur eine Zwischenstation auf dem Weg zu der eigentlichen Bestimmung des ETAS Demo Cars: Künftig werden angehende Mess- und Applikationsingenieure ihr komplexes Handwerk damit an modernsten ETAS-Tools erlernen. Dahinter steht die Überzeugung, dass optimale Ausbildung sichere, moderne Arbeitsplätze braucht. Gelebte Kooperationen mit Ausbildungsstätten und Hochschulen sind darum fester Bestandteil in der Unternehmensstrategie von ETAS.

Messen und Kalibrieren bei Versuchsfahrten

ETAS INCA-TOUCH erlaubt eine sichere Anzeige und Bedienung von INCA-Experimenten

Wegen des hohen Sicherheitsrisikos verbieten immer mehr Unternehmen die Bedienung von Laptops bei Testfahrten. Trotzdem müssen Ingenieure das Verhalten einzelner Fahrzeugfunktionen mithilfe von Messungen validieren und kalibrieren. Zu diesem Zweck lässt sich ETAS INCA sowohl per Touchscreen als auch mit Sprachbefehlen über die INCA-TOUCH-Schnittstelle bedienen.



INCA-TOUCH ist über den fest eingebauten Touchmonitor bedienbar (oben im Bild zu sehen).

Touch-Bedienung

Über INCA-TOUCH kann der Anwender die wesentlichen Mess- und Kalibrierfunktionen von INCA ausführen. Zur Anzeige von Messwerten und Einstellung von Kennwerten lassen sich Mess- und Kenngrößen von INCA-Experimenten spezifischen virtuellen Instrumenten zuordnen, die eigens für Touchscreens optimiert wurden.
Wird ein Laptop als INCA-Rechner verwendet, lässt sich das Eingabefenster auf einem zusätzlichen Touchscreen ausgeben. Bei Gebrauch eines Windows-Tablets kann dafür unmittelbar das Tablet-Display verwendet werden.

Hauptmerkmale

Sicher und bedienerfreundlich:

- Bedienung des Experiments, zum Beispiel Start / Stopp / Pause, Messdaten-Aufzeichnung, Starttrigger, Hardware-Initialisierung
- Anzeige der Messwerte in verschiedenen virtuellen Anzeigeinstrumenten, beispielsweise Oszilloskop, Balkendiagramm, Tabelle, Bit View, Kennlinie/Kennfeld, Tacho und LED
- Strukturierung von Bildschirminhalten zum Umschalten zwischen verschiedenen Teilexperimenten mithilfe von Layern

Automatisierungsfunktionen:

- Definition einzelner Kalibrierschritte, Ausführung durch Berührung eines Touch-Buttons
- Definition von Kalibrierprozeduren mit veränderbaren Wiederholintervallen und zugehörigen Dialogfenstern
- Wechsel zwischen alternativen Experimentierszenarien

Erweiterung der INCA-Funktionen:

- Bedienung durch Sprachbefehle zur Steuerung von Experimenten oder zur Kalibrierung von Kenngrößen
- Setzen von Markern während der Aufzeichnung mit der Option, gesprochene Kommentare zu ergänzen

A wie Allgäu – und Assistenzsysteme

ETAS unterstützt „A drive living lab“ an der Hochschule Kempten

Mit ihrem weltweit einzigartigen Masterstudiengang „Fahrerassistenzsysteme“ ist der Hochschule Kempten ein Coup gelungen. Studierende aus aller Welt stehen ebenso Schlange wie OEMs und Zulieferer, die sich in die Forschung des neuen „A drive living lab“ einklinken wollen. Koordinator Professor Stefan-Alexander Schneider erklärt im Interview, was es mit dem Lab auf sich hat und welche Rolle ETAS und ETAS ISOLAR-EVE darin spielen.

IM INTERVIEW

Prof. Dr. Stefan-Alexander Schneider ist Leiter des Masterstudiengangs Fahrerassistenzsysteme an der **Hochschule Kempten**.

RealTimes: Allgäu, autonomes Fahren und Assistenzsysteme – wie passt das zusammen?
Prof. Schneider: Wir haben hier an der Hochschule Kempten den weltweit einzigartigen Masterstudiengang „Fahrerassistenzsysteme“, an dem 15 Professoren aus drei Fakultäten beteiligt sind. Federführend ist dabei mein Lehrstuhl für Autonomes Fahren und Assistenzsysteme, den Continental Ende 2013 für fünf Jahre gestiftet hat. Es gibt in der Industrie hohen Bedarf an Systemingenieuren, die wissen, wie man Assistenzsyteme entwickelt. Wir bilden sie seit 2014 aus. Studienbewerber aus aller Welt rennen uns förmlich die Tür ein. Um so praxisnah wie irgend möglich auszubilden, haben wir jüngst unser „A drive living lab“ eröffnet.

RealTimes: Was hat es damit auf sich?
Prof. Schneider: Wir bilden auf 500 m² Fläche die gesamte Wertschöpfungskette der Assistenzsystem-Entwicklung nach, um unseren Studierenden unter Vorentwicklungsbedingungen die dafür notwendigen Prozesse, Methoden und Werkzeuge zu vermitteln. Und natürlich geht es auch darum, die Entwicklungsprozesse zu analysieren und zu optimieren. Elektrotechnik, Maschinenbau und Informatik arbeiten dabei Hand in Hand – und bringen ihre jeweilige Expertise ein.

RealTimes: Wofür steht das „A“ in „A drive living lab“?
Prof. Schneider: Allgäu, Assistenzsysteme und autonomes Fahren – wie Sie es eingangs aufgezählt haben. Aber es könnte auch „V-Lab“ heißen. Denn der Aufbau unseres Labors orientiert sich am V-Modell aus der Software- und Systementwicklung. Die Werkstatt misst 50 mal 10 Meter und stellt so ein gestrecktes V dar: Alle Schritte von der Anforderungsanalyse über die Funktions- und Systemspezifikation bis zu den vielfältigen Schritten der Validierung sind hier als Stationen aufgefädelt. Die Studierenden lernen und forschen also von Beginn an in industrieähnlicher Umgebung – ohne lange Wege. Dazu trägt auch ETAS bei, indem wir professionelle Werkzeuge, darunter ISOLAR-EVE zur Erzeugung virtueller Steuergeräte, das Hardware-in-the-Loop-System ETAS LABCAR und die Open-Source-Software BUSMASTER, zur Verfügung gestellt bekommen. Unsere Studierenden lernen so die Werkzeugketten kennen, mit denen sie auch in der Industrie arbeiten werden.

RealTimes: Welche Anwendungen schweben Ihnen mit den virtuellen Steuergeräten vor?
Prof. Schneider: Wir möchten damit unter anderem die Steuergeräte aus unterschiedlichen Domänen vernetzen. Für Fahrerassistenzsysteme ist das Zusammenspiel von Antriebs- und Fahrwerkssteuergeräten mit Sensorsystemen für die Umfelderkennung und -überwachung wichtig. Co-Simulation von Kamera-, Radar- oder Lidarsystemen mit virtuellen Steuergeräten oder auch im virtuellen Steuergeräteverbund ist dabei von zentralem Interesse. Es geht um ein tieferes Verständnis der Interaktion solcher Systeme, um Echtzeit-Datenkommunikation im Fahrzeug und perspektivisch auch um die Kommunikation zwischen Fahrzeugen und Infrastruktur. Hier ist Virtualisierung eine enorme Hilfe. Und natürlich müssen wir auch unsere heutigen Entwicklungsmethoden weiterentwickeln. Agile Software-Entwicklung ist der Trend. Nachträgliches Aufspielen von Funktionen, die trotz aller Flexibilität sauber validiert und verifiziert sein müssen. Solche Themen treiben die Industrie um. Das sieht man auch daran, dass sich schon unmittelbar nach der Gründung mehrere OEMs, Tier-1- und Tier-2-Zulieferer ins „A drive living lab“ eingeklinkt haben. In den nächsten Monaten wird die komplette Infrastruktur stehen. Dann werden wir hier richtig loslegen.

Hochschule Kempten
University of Applied Sciences

ISOLAR-EVE für die Virtualisierung von ADAS-Steuergeräten

Für die Virtualisierung von ADAS-Steuergeräten ist das Tool ISOLAR-EVE besonders gut geeignet, da es sämtliche Komponenten der Steuergeräte-Architektur berücksichtigt und damit das Verhalten des realen Steuergeräts auf dem PC sehr realitätsnah wiedergibt. So werden in die Virtualisierung sowohl Anwendungssoftware als auch die reale Basissoftware einschließlich einem vollständigen AUTOSAR-Betriebssystem einbezogen. Multi-Core-Konfigurationen werden realistisch abgebildet und heterogene Architekturen, bestehend aus Mikrocontrollern und Mikroprozessoren, können dargestellt werden. Auf diese Weise wird auch eine Simulation mehrerer vernetzter Steuergeräte und ihrer Kommunikation ideal unterstützt.

ETAS ISOLAR-B vervollständigt AUTOSAR-Toolkette

Mehr Informationen finden Sie unter www.etas.com/isolarb

ISOLAR-B macht den Steuergeräte-Integratoren das Leben leichter. Das neue Werkzeug zur Konfiguration von AUTOSAR-konformer Basissoftware nimmt ihnen viele Routineaufgaben ab. Mit einer klaren Darstellung, der Unterstützung für iterative Entwicklungsabläufe, einem hohen Automatisierungsgrad und der Möglichkeit zur frühen Validierung kommen sie schneller ans Ziel und die Qualität steigt.

Durch die intelligente Auswertung der Systeminformationen erkennen sie Zusammenhänge schneller. System-Extensions erlauben es, Lücken zwischen Systembeschreibung und Basissoftware-Konfiguration zu schließen und die Konfigurationsarbeit zu reduzieren. Zusammen mit ETAS ISOLAR-A und ETAS RTA-BSW (Basissoftware) entsteht eine nahtlos aufeinander abgestimmte AUTOSAR-Lösung, die sich schon in Projekten bewährt hat.

ISOLAR-A und ISOLAR-B, die beide das AUTOSAR-Release R4.3 unterstützen, nutzen eine gemeinsame Datenbasis. Dadurch werden Roundtrip-Zeiten verkürzt, die Konfiguration erleichtert und weiter automatisiert – das bedeutet noch mehr Effizienz in den Serienprojekten.
ISOLAR-B nutzt die Eclipse-Plattform und kann auf einfache Weise in bestehende Eclipse-Entwicklungsumgebungen integriert werden.

Neue Messmodulserie ES300

Die Messmodule der neuen ETAS-Produktfamilie ES300 lassen sich einfach miteinander verbinden.

Das ETAS-Messtechnik-Portfolio wurde in 2017 mit den kostengünstigen miniaturisierten Messmodulen der neuen Hardwareserie ES300 erweitert. Die wasser- und staubdichten Messgeräte können im Motorraum und am Chassis von Erprobungsfahrzeugen angebracht werden. Die Messdaten der Module werden über eine gemeinsame CAN-Leitung übertragen und können beispielsweise am Laptop in Kombination mit den USB-CAN-Schnittstellenmodulen ES581.4 oder ES584 zeitsynchron zu CAN-Signalen von Steuergeräten mit ETAS INCA erfasst werden. Aktuell stehen das Thermo-Modul ES321 mit acht, das A/D-Modul ES313 und das Zähler- und Frequenzmodul ES341 mit jeweils vier Kanälen zur Verfügung. Bei den Geräten ES313 und ES341 sind zusätzlich pro Kanal getrennte Versorgungen für die angeschlossenen Sensoren berücksichtigt.

Testsysteme effizienter skalieren

Um eine bessere Skalierbarkeit der ETAS-LABCAR-HiL-Testsysteme zu erzielen, hat ETAS neue elektromechanische und elektronische Systemkomponenten entwickelt, die bereits mit großem Erfolg in Kundenprojekten eingesetzt werden. Damit lassen sich sowohl Einzelsteuergeräte-Testsysteme darstellen als auch HiL-Prüfstände für die System- und Gesamtfahrzeugvalidierung flexibel konfigurieren.
Als zentrale Baugruppen werden Einschubkarten der PCI-Express-Plattform ES5300 in 60 oder 80 cm breite 19-Zoll-Racks mit einer Höhe von 24, 33 oder 38 Einheiten eingebaut. Bei den Racks mit 80 cm Außenmaß sind 24 Positionen vorgesehen, an denen Steckverbinder mit bis zu 300 Einzelkontakten zum Anschluss von Steuergeräten und Lasten angebracht werden können. Die interne Verkabelung wird längenoptimiert auf seitlich angebrachten, innenliegenden Panels geführt. Daran können bei Bedarf Umschalter für Signalpfade und spezifische Module montiert werden, wie zum Beispiel Module zur hochgenauen Messung von Standby-Strömen oder anderen Versorgungs- und Laststrom. Die auf Basis dieser Komponenten aufgebauten LABCAR-Systeme sind konform zu den IEC 61326-1-Vorgaben zur Elektromagnetischen Verträglichkeit (EMV). Zusätzlich zur Minimierung der Signalverzögerungen im geschlossenen Regelkreis wurde beim Layout der Leiterplatten der ES53xx-I/O-Karten auch die EMV besonders beachtet.
Die Freigabe der ausgelieferten Systeme erfolgt konform zur Sicherheitsnorm IEC 61010-1, was beispielsweise den Einsatz brandhemmender Bauteile und die Prüfung des mechanischen und elektrischen Berührungsschutzes umfasst.

Das neue Drive-Rekorder-Modul ES820 des ETAS-Systems ES800.

Neuer Drive-Rekorder ES820

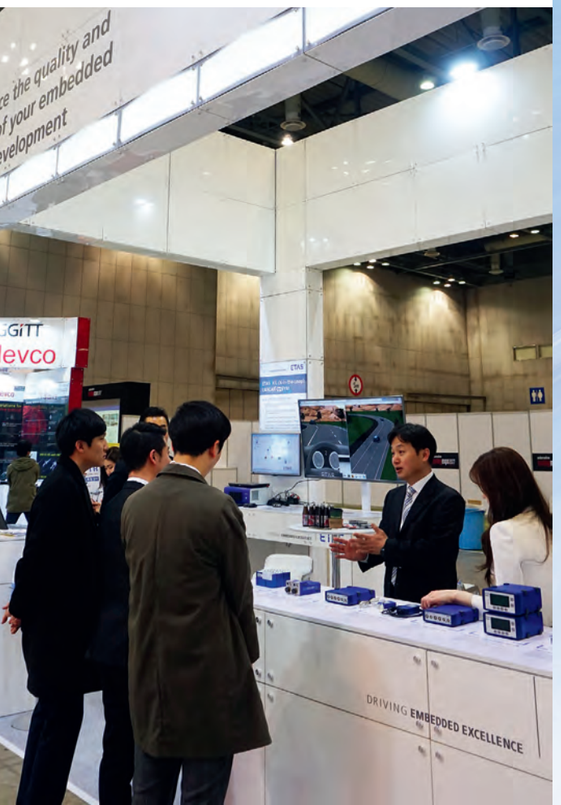
Seit September steht das Drive-Rekorder-Modul ES820 des neuen ETAS-Systems ES800 zur Verfügung. Das Modul ersetzt den INCA-PC oder Laptop und kann für eine Vielzahl von Messaufgaben in der Entwicklung, Applikation und bei der Validierung von elektronischen Systemen im Fahrzeug eingesetzt werden. In Kombination mit ES89x- und ES5xx-Schnittstellenmodulen lassen sich Steuergeräte mit ETK-, XETK- oder besonders leistungsfähigen FETK-Schnittstellen sowie mehrere LIN-, CAN/CAN FD- und FlexRay-Busse an den Drive-Rekorder anschließen. Mithilfe von Messmodulen der Serien ES400 und ES600 können Signale aus der Fahrzeugumgebung mit hoher Rate erfasst werden. Zusätzlich zum internen Solid State Drive (SSD) mit einer Speicherkapazität von 128 GB stehen einfach austauschbare SSD-Speichermodule mit Kapazitäten von wahlweise 500 GB oder 1 TB zur Aufzeichnung von Messdaten zur Verfügung.

Ein Jahr in ETAS-Bildern

ETAS Brasilien war auf dem **internationalen Symposium für Automobiltechnik (SIMEA)** in Saõ Paulo vertreten. Im Fokus: Skalierbare Testlösungen – Von Desktop- bis zu Netzwerksystemen, Validierung von Fahrzeugen und Messlösungen.

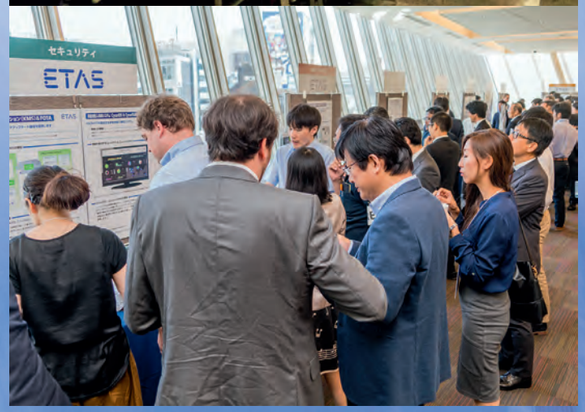
ETAS-Stand auf der **Automotive Testing Expo 2017** in Stuttgart mit den Schwerpunktthemen Skalierbare Testlösungen – Von Desktop- bis zu Netzwerksystemen, Validierung von Fahrzeugen und Messlösungen.

ETAS Korea präsentierte Lösungen auf der **Automotive Testing Expo 2017** in Seoul. Im Fokus: XiL (X-in-the-Loop), Messlösungen.



ETAS und ESCRYPT zeigten auf der **embedded world** in Nürnberg Lösungen zur Software-Entwicklung sowie Safety und Security. Ein Highlight war das ETAS Demo Car, ausgestattet mit INCA-TOUCH und ETAS-Hardware.

ETAS Japan veranstaltete im September 2017 das 9. Symposium **Automotive Embedded Systems Development 2017** in Tokio. Es stand unter dem Motto „Challenges for the Future and Beyond“. Rund 420 Kunden nahmen am ETAS-Symposium teil.



ETAS UK nahm zusammen mit Bosch am **Cenex Low Carbon Vehicle Event** in Millbrook, Großbritannien, teil. Ein Highlight war auch hier das ETAS Demo Car, ausgestattet mit INCA-TOUCH und ETAS-Hardware.

Neuer Standort in Japan

Rund 40 Kunden und Partner nahmen im Februar an den Eröffnungsfeierlichkeiten des neuen Standorts im japanischen Nagoya mit anschließendem Dinner teil. Fünf Field Application Engineers und zwei Key Account Manager werden ETAS dabei unterstützen, die Geschäftsbeziehungen im Westen von Japan auszubauen – ein Gebiet, das eine Schlüsselrolle in der Automobilindustrie innehat. „Mit dem neuen Büro in Nagoya kann ETAS die Marktanforderungen erfüllen und Trends in Japan adressieren. Die Lösungen und Dienstleistungen von ETAS ermöglichen einen Qualitäts- und Effizienzsprung in der Entwicklung und Pflege von Embedded Systemen", sagte Friedhelm Pickhard, Vorsitzender der Geschäftsführung der ETAS GmbH, in seiner Eröffnungsrede. Für ETAS ist dies ein wichtiger Schritt, um die erfolgreichen Geschäftsaktivitäten in Japan und der Automobilindustrie weiter gedeihen zu lassen.

Am 17. Februar 2017 fand die feierliche Eröffnung des neuen ETAS-Standorts in Nagoya statt.

AUTORIN

Anja Krahl ist als Pressesprecherin verantwortlich für die Presse- und Öffentlichkeitsarbeit bei der **ETAS GmbH**.

ETAS übernimmt TrustPoint

Die Übernahme der TrustPoint Innovation Technologies, Ltd. stärkt das Cyber-Security-Portfolio von ETAS und unterstützt die Wachstumsstrategie durch Safety- und Security-Lösungen für Embedded Systeme mit begrenzten Ressourcen in vernetzten Fahrzeugen und dem Internet der Dinge (IoT). TrustPoint Innovation Technologies, Ltd. ist spezialisiert auf Datensicherheitslösungen für Vehicle-to-X-(V2X-)Anwendungen sowie für den Bereich sicherer Machine-to-Machine-(M2M-)Kommunikation im Internet der Dinge. Das akquirierte Unternehmen wird in die ETAS Embedded Systems Canada Inc. mit Sitz in Waterloo, Ontario, integriert, die gemeinsam mit der ETAS-Tochtergesellschaft ESCRYPT GmbH auf Sicherheitslösungen für Embedded Systeme spezialisiert ist.

Sherry Shannon-Vanstone, President und CEO von TrustPoint Innovation Technologies, Ltd., und David MacFarlane, Managing Director ETAS Embedded Systems Canada Inc., nach der Vertragsunterzeichnung.

escar USA 2017

Reger Austausch zwischen Industrie, Wissenschaft und Behörden

ETAS und ESCRYPT begrüßten dieses Jahr auf der escar USA (Embedded Security in Cars) zum fünften Mal ein internationales Fachpublikum, mit dem sie die neuesten Entwicklungen im Kampf gegen Risiken, Bedrohungen und Schwachstellen im Bereich Cyber-Security in Fahrzeugen diskutierten.

Die zweitägige Konferenz, die am 21. und 22. Juni 2017 in der Nähe von Detroit (US-Bundesstaat Michigan) stattfand, startete 2003 als kleiner Fachworkshop in Köln. Seither wird sie jährlich in Europa und zusätzlich seit 2013 in den USA beziehungsweise seit 2014 in Asien veranstaltet.

Die escar USA stellt ein Forum bereit, um die Zusammenarbeit von Privatindustrie, Wissenschaft und Regierungsbehörden im Hinblick auf aktuelle Cyberbedrohungen in Fahrzeugen sowie entsprechende Gegenmaßnahmen zu fördern.

Hierfür kamen bei dem Event über 300 unterschiedlichste Teilnehmer aus den drei genannten Bereichen zusammen, um über die aktuellsten Ansätze für die Cyber-Security in Fahrzeugen zu sprechen.

Auch die 19 Redner hatten entsprechend vielfältige Hintergründe. Als Erster erläuterte Paul Rosenzweig von Redbranch Law and Consulting über das sich wandelnde Haftungsrecht im Bereich der Cyber-Security. Die anderen Präsentationen drehten sich unter anderem um kontextabhängige Angriffserkennung in Automotive-Steuerungen, Entropie und Zufälligkeit in Fahrzeugumgebungen und V2X-Anwendungen sowie um Risiko- und Sicherheitsbewertung von Mobilverbindungen in Fahrzeugen. Um ein hohes Niveau zu erreichen, gibt es ein sorgfältiges Auswahlverfahren. Dazu reichen die Redner ihre Vorträge im Blindverfahren bei dem Programmkomitee ein und jede einzelne Präsentation wird anschließend unabhängig von mindestens drei Mitgliedern des Komitees geprüft. Dieses Jahr schafften es mit 27 Prozent nur circa ein Viertel der Einsendungen ins Konferenzprogramm.

Neben den Vorträgen nimmt auch das Networking einen wichtigen Raum in der Veranstaltung ein – erst bei einem Cocktailempfang nach den Präsentationen und später bei einem Abendessen im Freien, dem sich die Teilnehmer bis spätabends austauschten und Marshmallows über dem offenen Feuer grillten.

Das Feedback der Teilnehmer war überaus positiv, ein Gast verglich die escar sogar mit der Ansprache zur Lage der Nation in den USA: „Die escar gilt mittlerweile als Ansprache zur Lage der Cyber-Security in Fahrzeugen. Weiter so!"

Das werden wir für die Planung der escar USA 2018 im Hinterkopf behalten.

Die escar USA 2018 findet vom 20. bis 21. Juni 2018 statt.
Weitere Informationen finden Sie unter www.escar.info/escar-usa

Mitarbeiter von ETAS, ESCRYPT und TrustPoint Innovation Technologies, Ltd. führten gemeinsam durch die escar USA 2017.

AUTORIN

Claudia Hartwell ist Senior Marketing Specialist Communications bei **ETAS Inc.** in Ann Arbor, Michigan, USA.

Zehn Jahre ETAS Automotive India

AUTOREN

Sameera C Damle ist Leiter des Bereichs Technical Sales und Engineering Solutions bei **ETAS Automotive India Pvt. Ltd.** in Bengaluru.

Rashmi Rao ist Produktmanagerin für Engineering Test Solutions bei **ETAS Automotive India Pvt. Ltd.** in Bengaluru.

ETAS Indien feierte dieses Jubiläum zusammen mit seinen wichtigsten Wegbegleitern: seinen Kunden. Am 2. August blickten in Bengaluru 50 Führungskräfte auf Kundenseite gemeinsam mit ETAS in die Vergangenheit und in die Zukunft. Das ETAS-Management repräsentierten Friedhelm Pickhard, Vorsitzender der Geschäftsführung der ETAS GmbH, Wolfgang Sienel, Vice President ETAS Sales Asia-Pacific, und Mahavir Patil, General Manager ETAS India.

Die Veranstaltung begann mit der traditionellen indischen „Lamp Lighting Ceremony", bei der als Symbol für den Weg in eine strahlende Zukunft eine Lampe angezündet wird. Danach folgte das Anzünden einer „digitalen Lampe" auf einem LED-Bildschirm – als Fortführung der Tradition, aber mit High-Tech-Kniff. Nach der Begrüßung der Gäste durch Mahavir Patil wurden die zahlreichen Meilensteine und Erfolge von ETAS Indien durch ein Video verdeutlicht. Friedhelm Pickhard erläuterte anschließend, wie ETAS die Zukunft der automobilen Software-Entwicklung beurteilt.

Bei einer Fragerunde mit Kunden sprach das ETAS-Management über verschiedene Themen wie die neue Abgasnorm Bharat Stage 6 (BS6), die Indien 2020 einführt, Elektrifizierung in Indien und anderen Ländern sowie Embedded Security.

Die traditionelle „Lamp Lighting Ceremony".

Während der Fragerunde (v. l. n. r.): Wolfgang Sienel, Vice President ETAS Sales Asia-Pacific, Friedhelm Pickhard, Vorsitzender der Geschäftsführung der ETAS GmbH, und Mahavir Patil, General Manager ETAS India.

ETAS Indien feiert zusammen mit Kunden das zehnjährige Bestehen

2017 ist ein bedeutendes Jahr für ETAS Indien. Als die Niederlassung 2007 eröffnete, lieferte sie mit drei Mitarbeitern Mess- und Applikationslösungen an zwei indische Kunden. Mittlerweile beschäftigt ETAS Indien 40 Mitarbeiter und bietet Lösungen aus dem gesamten ETAS-Portfolio an. Zu den 150 Kunden im Land zählen einheimische OEMs wie Mahindra, Tata Motors, Force Motors, Bajaj und Hero Honda sowie die indischen Niederlassungen der wichtigsten internationalen Tier-1-Zulieferer und OEMs wie Maruti Suzuki India Limited, Hyundai, Volkswagen, Renault, Nissan, Honda, Continental, Delphi, Denso, John Deere und EATON.

Um den Kunden eine klare Vorstellung davon zu geben, wie sich ETAS den wichtigsten sich abzeichnenden Megatrends stellt, wurde ein „Technology Theatre" organisiert. Hier präsentierten Experten von ETAS Indien zukünftige ETAS-Lösungen aus den folgenden fünf Kernbereichen: Fahrerassistenzsysteme (ADAS), Big Data, Virtualisierung, Elektrifizierung sowie sichere Software. Die Kunden waren sehr daran interessiert zu erfahren, wie ETAS die Zukunft einschätzt und diskutierten mit den Technikexperten von ETAS lebhaft über die geplanten Lösungen.

Vor dem abschließenden Abendessen konnten die Teilnehmer ihre musikalische Ader an einer afrikanischen Trommel (namens Djemble) ausleben. Das gemeinsame Trommeln unter der Leitung der Schlagzeuger von Taal Inc. sorgte beim Publikum für großen Spaß und zauberte allen ein Lächeln aufs Gesicht – die richtige Stimmung für das anschließende Cocktaildinner.

Nach zehn Jahren kann sich das junge Team von ETAS Indien definitiv auf viele weitere Jahrzehnte freuen und gemeinsam Embedded Excellence in Indien weiter vorantreiben.

Persönlich und nah

Customer Support bei ETAS

Bei ETAS wird ausgezeichneter Support auch nach Auslieferung der Produkte großgeschrieben. Vor allem die persönliche Bindung ist dabei sehr wichtig, denn so kann auf individuelle Fragen noch detaillierter eingegangen werden.

AUTOREN

Selina Epple ist Redakteurin bei der **ETAS GmbH**.

Hans-Jürgen Schmidt-Fürst ist Director Global Customer Support bei der **ETAS GmbH**.

Norbert Seidler ist Specialist Support Engineering bei der **ETAS GmbH**.

Wer kennt die Situation nicht? Man benötigt schnell Hilfe bei der Bedienung eines Tools, findet aber keine Telefonnummer oder E-Mail-Adresse des Anbieters. Stattdessen hangelt man sich mühsam durch ein Standardformular, welches allerdings nur begrenzt geeignet ist, das Problem zu erfassen. Die Antwort erhält man oft erst zwei Tage später und die darin enthaltene Lösung ist meist nur bedingt zufriedenstellend.

Entgegen diesem Trend, den Support immer mehr zu anonymisieren und auf Sprachcomputer, Avatare oder künstliche Intelligenz zu setzen, steht beim ETAS-Support weiterhin der Mensch im Vordergrund. Aus der jährlichen ETAS-Befragung zur Kundenzufriedenheit geht eindeutig hervor, dass gerade der persönliche Kontakt als Mehrwert angesehen und von den Kunden sehr geschätzt wird. Auch wenn ETAS an zusätzlichen Supportkanälen arbeitet – die Kundennähe bleibt oberste Priorität.

Schnell und unkompliziert – Erfolgreicher Support als Teamleistung

An allen ETAS-Standorten wird ein qualitativ hochwertiger Telefon- und E-Mail-Support angeboten. Die überwiegende Anzahl an Support-Anfragen kann in der Regel innerhalb kürzester Zeit gelöst werden. Dies liegt insbesondere an den vielen hervorragend qualifizierten Mitarbeitern mit langjähriger Erfahrung. Erfolgreicher Kundensupport ist bei ETAS eine Teamleistung, die insbesondere durch Spezialisierung der einzelnen Mitarbeiter auf die Themen des ETAS-Portfolios erreicht wird. Mit diesen Experten gelingt es dem Team, unterschiedliche Support-Level zu bedienen.

- First-Level-Support: Problemannahme und Lösung von Anfragen, die schnell und direkt zu lösen sind
- Second-Level-Support: Nachgelagerter Support, der auf bestimmte Themen spezialisiert ist und die Anfragen abarbeitet, die der First-Level-Support nicht direkt am Telefon lösen kann
- Third-Level-Support: Für spezielle Anfragen und komplexe Anforderungen

Das Expertenwissen wird intern in Wiki-Datenbanken dokumentiert und seit letztem Jahr auch in Form von FAQs extern zur Verfügung gestellt. Die gefragten FAQs sind im Download Center der ETAS-Website abrufbar.

Nah am Kunden

Zusätzlich zur Hotline bietet ETAS auch den Support vor Ort beim Kunden an. Die Resident Engineers von ETAS sind geschätzte Ansprechpartner. Neben der Anwendung der Produkte stehen bei deren Arbeit auch die effiziente und zügige Integration in die Kundenprozesse und Toollandschaft im Vordergrund.

Jedoch leisten nicht nur die vom Kunden beauftragten Resident Engineers Support vor Ort. So oft wie möglich besuchen auch die ETAS-Hotline-Experten die Kunden. Dadurch wird nicht nur die Kundenbindung erhöht, sondern auch die ETAS-internen Kenntnisse über die Arbeitsweise der Kunden stetig verbessert. Somit wird die Support-Qualität zusätzlich gesteigert und die Arbeit der Hotline-Mitarbeiter abwechslungsreicher – ebenfalls eine wichtige Voraussetzung für qualitativ hochwertige Arbeit.

On the road – Teststrecken-Support

In den letzten Jahren waren die ETAS-Support-Ingenieure darüber hinaus gern gesehene Begleiter bei vielen Erprobungen unter anderem in Schweden oder Südafrika. Ein besonderes Highlight ist der Teststrecken-Support in der spanischen Provinz Granada, den ETAS seit mehreren Jahren für drei bis vier Wochen im Jahr in Eigenregie ausrichtet. Mit großen Temperaturdifferenzen und Höhenunterschieden von bis zu 2.600 Metern bieten die Berge der Sierra Nevada den Fahrzeugherstellern ideale Voraussetzungen, ihre Autos auf Herz und Nieren zu prüfen.

Daher ist es nicht verwunderlich, dort viele Fahrzeughersteller und Zulieferer anzutreffen, die den ETAS-Support gerne in Anspruch nehmen. Die äußerst positiven Kundenrückmeldungen motivieren das ETAS-Support-Team, den eingeschlagenen Weg weiterzugehen und trotz aller technischen Trends den Fokus auf den persönlichen Kontakt zu legen.

Theorie trifft auf Realität – Use Cases

Ein weiterer Bestandteil des ETAS-Serviceangebots sind die Use Cases, auffindbar im Download Center der ETAS-Website. Diese zeigen interessante Anwendungsfälle sowie Tipps und Tricks und sind von Anwendern für Anwender geschrieben. Sie enthalten eine selbsterklärende Do-it-yourself-Anleitung und zeigen, wie man ETAS-Tools anwenden und welche Probleme man damit lösen kann. Somit ermöglichen sie eine optimale Nutzung der Tools über Standardsituationen hinaus. Die Anwendungsfälle stammen meistens aus Erfahrungen in Kundenprojekten, aus Workshops mit Kunden sowie aus konkreten Kundenanfragen. Somit werden relevante Themen direkt aus dem Arbeitsalltag aufgegriffen. ETAS stellt sie mit eigener Hardware und eigenen Daten nach, damit keinerlei Rückschluss auf den Kunden möglich ist, von dem der ursprüngliche Anwendungsfall stammt.

Es lässt sich festhalten: Unabhängig davon, wo und in welcher Form – ETAS steht seinen Kunden jederzeit mit Rat und Tat zur Seite!

Zusammenarbeit zwischen ETAS und Lynx Software Technologies

ETAS und Lynx Software Technologies kooperieren, um eine gemeinsame, sichere Steuergeräte-Plattformtechnologie bereitzustellen, welche die Anforderungen der nächsten Generation vernetzter und autonomer Fahrzeuge erfüllt. Vereint werden die Erfahrung bei der Entwicklung von sicherheitskritischen Automobilanwendungen und höchster Cyber-Security. Für die nächste Generation vernetzter und autonomer Fahrzeuge müssen leistungsstarke Domain-Controller (DC-ECU) und Fahrzeugcomputer (VC-ECU) in die EE-Architektur eingeführt werden. Die DC/VC-ECUs werden leistungsstarke Mikroprozessoren mit vielfältigeren, anpassungsfähigeren Softwareplattformen verwenden, die auch weiterhin hohe Anforderungen an funktionale Sicherheit, Cyber-Security und Echtzeit-Verarbeitung haben und in die klassischen Plattformen integrierbar sein müssen. Die gemeinsame Lösung bietet die zuverlässige, sichere Softwaregrundlage, die DC/VC-ECUs benötigen.

STMicroelectronics, ETAS und ESCRYPT: sichere Anwendungen für das vernetzte Auto

Die Kooperation mit STMicroelectronics (New York Stock Exchange: STM), einem führenden Hersteller von Halbleitern für Elektronikanwendungen, hat zum Ziel, eine komplette Plattform mit Mikrocontrollern, Softwaretools und Sicherheitslösungen bereitzustellen, die die Entwicklung neuer Fahrzeugsteuergeräte für das Zeitalter des vernetzten Autos beschleunigt. Sie erlaubt Zulieferern, sichere Steuergeräte zu konstruieren, die bei Fernzugriff über verschiedene Netzwerke einen hohen Schutz der Privatsphäre der Fahrzeughalter, des geistigen Eigentums der OEMs und der funktionalen Integrität der Steuergeräte gewährleisten. Die gemeinsame Lösung basiert auf energieeffizienten, echtzeitfähigen Automotive-Mikrocontrollern der SPC58-Serie von STMicroelectronics. Sie umfasst ein integriertes Hardware-Sicherheitsmodul (Hardware Security Module, HSM), mehrere hochmoderne CAN FD-Schnittstellen, LIN, FlexRay und Ethernet mit Zeitstempel. Dazu gehören auch Secure Elements und eingebettete SIM-Karten (Subscriber Identity Modules), die vor Internetangriffen auf Steuergeräte und Gateways schützen. ESCRYPT sorgt für eine sichere Steuergerätekommunikation, darunter die Verteilung von Over-the-Air-Software-Updates (OTA), und stellt Firmware und Middleware für Steuergeräte-Entwickler bereit, damit diese das SPC58-HSM nutzen können. Das HSM und die Sicherheitstechnologie von ESCRYPT sorgen gemeinsam für die erforderliche Authentifizierung vertrauenswürdiger Quellen und den Schutz vor unbefugtem Zugriff. Von ETAS sind die bewährten RTA-Softwareprodukte für die Entwicklung von Steuergerätesoftware im Einsatz. RTA-BSW (Basissoftware) wird durch die Tools ETAS ISOLAR-A und ETAS ISOLAR-EVE ergänzt, mit denen der Nutzer einen kompletten Steuergeräte-Software-Stack in einer virtuellen Umgebung entwickeln und testen kann.

Renesas Electronics und ESCRYPT kooperieren

Renesas Electronics Corporation, ein führender Hersteller hochmoderner Halbleiterlösungen, und die ETAS-Tochtergesellschaft ESCRYPT arbeiten gemeinsam an einer neuen Plattformlösung für einfachere Security-Integration bei komplexen Automotive-Anwendungen für das autonome Fahren.

Bei der neuen kombinierten Hard-/Softwareplattform werden die Automotive-Safety-Mikrocontroller (MCUs) der RH850/P1x-C-Reihe von Renesas, welche funktionale Sicherheit, Security und Netzwerktechnologien auf einem Chip vereinen, mit ESCRYPTs Security-Software-Stack für Hardware-Security-Module, CycurHSM, verbunden. Hierdurch werden hochkomplexe Security-Lösungen für Fahrzeuge ermöglicht und Entwicklungszeiten verkürzt. Zudem wirkt die neue Plattformlösung als Beschleuniger des autonomen Fahrens, indem sie es erlaubt, die erforderlichen Safety- und Security-Funktionen schneller zu verwirklichen.

AUTORIN

Anja Krahl ist als Pressesprecherin verantwortlich für die Presse- und Öffentlichkeitsarbeit bei der **ETAS GmbH**.

ETAS-Standorte weltweit

Deutschland
Stuttgart
(Unternehmenszentrale)

Brasilien
São Bernardo do Campo

Frankreich
Saint-Ouen

Großbritannien
Derby
York

Indien
Bengaluru
Chennai
Gurgaon
Pune

Italien
Turin

Japan
Nagoya
Utsunomiya
Yokohama

Kanada
Waterloo, Ontario

Korea
Seongnam-Si

Schweden
Göteborg

USA
Ann Arbor, Michigan

VR China
Changchun
Chongqing
Guangzhou
Peking
Shanghai
Wuhan

ETAS GmbH, Borsigstraße 14, 70469 Stuttgart · **Geschäftsführung:** Friedhelm Pickhard, Bernd Hergert, Christopher White **Aufsichtsratsvorsitzender:** Dr. Walter Schirm · **Sitz:** Stuttgart · **Registergericht:** Amtsgericht Stuttgart HRB 19033

Redaktionsleitung: Tatiana Bohlmann · **Redaktion:** Nicole Bruns, Jürgen Crepin, Claudia Hartwell, Anja Krahl, Silke Kronimus, Dr. Ulrich Lauff, Andrea Müller · **Autoren dieser Ausgabe:** Dr. Darren Buttle, Wonseok Chang, Yooshin Cho, Jürgen Crepin, Sameera C Damle, Dr. James Dickie, Selina Epple, Norbert Fabritius, Marius Feilhauer, Klaus Fronius, Randy Gutsche, Dr. Jürgen Häring, Claudia Hartwell, Michael Hauser, Dr. Jan Holle, Jochen Horinek, Ramona Jung, Dr. Markus Kögel, Anja Krahl, Dr.-Ing. Tobias Kreuzinger, Dr. Ulrich Lauff, Rao Rashmi, Rajesh Reddy, Hans-Jürgen Schmidt-Fürst, Norbert Seidler, Jörg Spranger, Dr. Christoph Stoermer, Dr. Nigel Tracey, Peter Trechow, Deepa Vijayaraghavan, Dr.-Ing. Marko Wolf, Wongeun Yoo · **Folgende Beiträge erschienen bereits als Langversion in:** Elektronik automotive, (S. 5-7, S. 8-11); Hanser automotive (S. 14, S. 30-31), ATZelektronik (S. 12-13, S. 32-34), Automobil Elektronik (S. 26-27), ATZextra (S. 28-29) · **Gestaltung und Produktionsleitung:** vogt grafik · **Übersetzungen:** Burton, Van Iersel & Whitney GmbH · **Druck:** Gmähle-Scheel Print-Medien GmbH · **Auflage:** Deutsch, Englisch, Japanisch: 13.800 · **Bildnachweise:** DKG Photography, ESCRYPT, ETAS, fotolia, FSG Schulz, Hochschule Kempten, Hyundai R&D Center, iStockphoto, René Müller Photographie, Robert Bosch GmbH, shutterstock

Unser Newsletter **RealTimes online** ergänzt die gedruckte Ausgabe des RealTimes-Magazins. In regelmäßigen Abständen informieren wir Sie darin über aktuelle Themen aus der ETAS-Welt:

- Anwendungsfälle und Erfolgsgeschichten mit ETAS-Produkten
- Technische Beiträge
- Unternehmensinformationen
- Veranstaltungs- und Trainingshinweise
- Interviews
- FAQs

Hier geht's zum Anmeldeformular und zu den bisher erschienenen Ausgaben von **RealTimes online**:

www.etas.com/RTo