

AUTOREN



MICHAEL GLASS
arbeitet am Lehrstuhl für Hardware-Software-Co-Design an der Universität Erlangen-Nürnberg in Erlangen.



DR.-ING. DANIEL HERRSCHER
arbeitet am Thema IP-basiertes Bordnetz bei der BMW Forschung und Technik GmbH in München.



HERBERT MEIER
arbeitet im Bereich Advanced Development and Innovations – Infotainment & Connectivity bei der Continental Automotive GmbH in Regensburg.



DR. MARTIN PIASTOWSKI
arbeitet im Bereich Corporate Sector Research and Advance Engineering bei der Robert Bosch GmbH in Stuttgart.

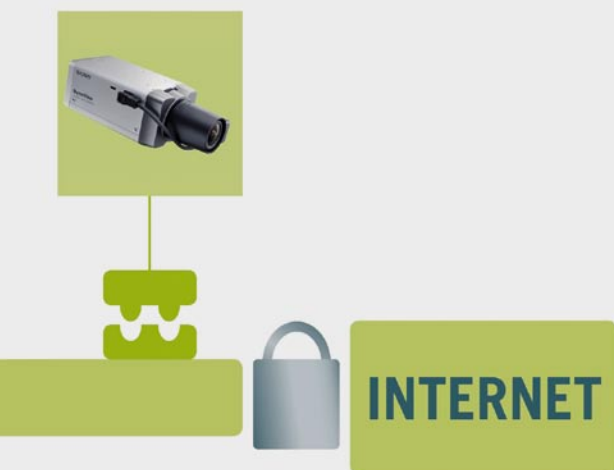


PETER SCHOO
leitet den Forschungsbereich Netzsicherheit und Frühwarnsysteme am Fraunhofer-Institut für Sichere Informationstechnologie SIT in Garching bei München.



„SEIS“ – SICHERHEIT IN EINGEBETTETEN IP-BASIERTEN SYSTEMEN

Die stetig steigende Variantenvielfalt der Vernetzungstechnologien, die heute in Automobilen eingesetzt werden, führt zu komplexen und kostenintensiven E/E-Architekturen. Die Innovationsallianz Automobilelektronik EIENOVA hat deshalb das Forschungsprojekt „SEIS – Sicherheit in Eingebetteten IP-basierten Systemen“ initiiert. Ziel ist eine durchgängige Sicherheitslösung für die Internet-Protokoll-basierte Kommunikation innerhalb des Fahrzeugs und die Kommunikation des Fahrzeugs mit der Umwelt. Die Projektpartner berichten erstmals über die Erfolge der vor einem Jahr gestarteten Sicherheitsoffensive.



1	EINLEITUNG
2	DAS PROJEKT SEIS
3	TEILPROJEKT IP-BASIERTE NETZE
4	TEILPROJEKT SYSTEMSOFTWARE / MIDDLEWARE
5	TEILPROJEKT SICHERHEIT
6	TEILPROJEKT BEWERTUNG UND OPTIMIERUNG
7	DIE DEMONSTRATOREN
8	FAZIT

1 EINLEITUNG

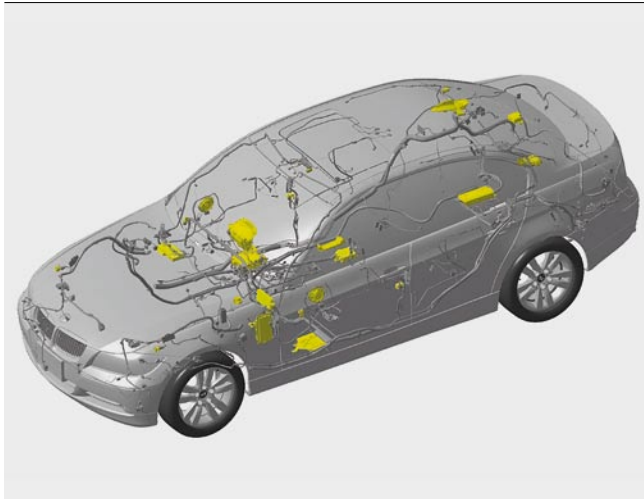
Ein aktuelles Fahrzeug verfügt über eine komplexe Kommunikationsinfrastruktur. Bis zu 70 elektronische Steuergeräte (ECUs) kommunizieren über bis zu fünf verschiedene Vernetzungstechnologien, ❶, die über Gateways miteinander verbunden sind. Auch außerhalb des Fahrzeugs existiert eine Vielzahl unterschiedlicher Vernetzungstechnologien. Durch die speziellen, meist nicht direkt kompatiblen Protokolle werden Innovationen erschwert, die zusätzliche Kommunikation dieser Geräte erfordern. Durch die Verwendung des Internet Protokolls (IP) als einheitliche, domänenübergreifende Kommunikationsschicht im Fahrzeug soll dieser Innovationsstau gelöst werden.

Der Fokus der Forschungsarbeit „SEIS – Sicherheit in Eingebetteten IP-basierten Systemen“, liegt dabei auf dem Thema Sicherheit. Hilfreich ist hierbei ein einheitlicher Kommunikationsstandard, der die Komplexität der Vernetzung im Fahrzeug reduziert und so die Betriebssicherheit nachhaltig steigert. Neben der Safety wird im Projekt SEIS besonders die Security betrachtet, die Sicherheit gegen nicht autorisierte Zugriffe und Manipulationen. Je stärker das Fahrzeug in die Umwelt integriert ist, desto höher sind die Anforderungen, die an die Sicherheit gestellt werden müssen.

2 DAS PROJEKT SEIS

Das Projekt SEIS der Innovationsallianz Automobilelektronik (EINOVA) [1] wird vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des IKT2020 und der High-Tech Strategie der Bundesregierung gefördert. Die Laufzeit beträgt drei Jahre, es steht ein Gesamtbudget von 18 Millionen Euro zur Verfügung. Beteiligt sind die Unternehmen Alcatel-Lucent Deutschland AG, Audi AG, Audi Electronics Venture GmbH, BMW AG, BMW Forschung und Technik GmbH, Continental Automotive GmbH, Daimler AG, EADS Deutschland GmbH, Elektrobit Automotive GmbH, Infineon Technologies AG, Robert Bosch GmbH, Volkswagen AG, die Universitäten Erlangen-Nürnberg und Karlsruhe, sowie die TU Chemnitz und die TU München, die Fraunhofer-Einrichtung für Systeme der Kommunikationstechnik ESK und das Fraunhofer-Institut für Sichere Informationstechnologie SIT. Die BMW Forschung und Technik GmbH in München koordiniert das Gesamtprojekt.

Das Verbundvorhaben gliedert sich in sechs Teilprojekte (TPs), ❷. Aufbauend auf die in Teilprojekt 1 (TP 1) entwickelten Anforderungen an das Kommunikationssystem werden in den weiteren Teilprojekten mögliche Lösungen erforscht und abschließend in TP 6 in Form von Demonstratoren erlebbar gemacht. Die erwarteten Herausforderungen und mögliche Lösungsansätze von TP 2 bis 6 sind im Folgenden dargestellt.



1 Steuergeräte in einem Fahrzeug (stark vereinfacht)

3 TEILPROJEKT IP-BASIERTE NETZE

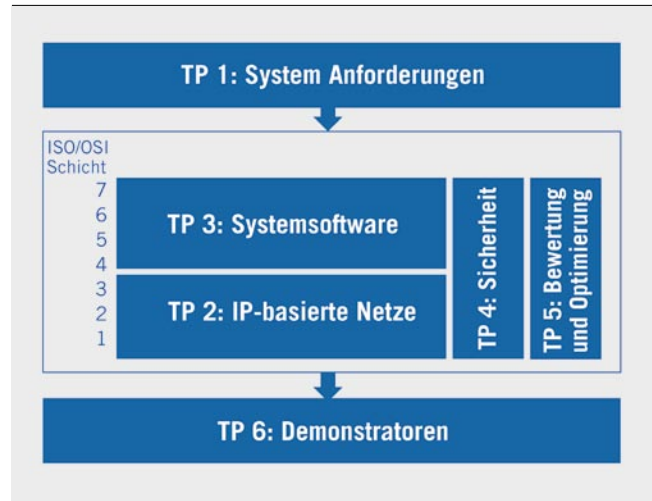
Das Ziel dieses Teilprojekts ist es, die technischen Grundlagen zu schaffen, um IP-basierte Netze in großem Umfang im Automobil einsetzbar zu machen. Dabei werden sicher nicht alle aktuell im Fahrzeug vorhandenen Kommunikationstechnologien abgelöst werden. Ein realistisches Ziel ist es aber, einige der heutigen Technologien in einem IP-basierten Netz weiter zu verwenden, und nur wo nötig neue Technologien einzusetzen. Auch hier ist keine vollständige Eigenentwicklung der Automobilindustrie geplant. Im Idealfall kann auf bewährte Technologien zurückgegriffen werden, die bereits in anderen Industriezweigen in großer Stückzahl eingesetzt werden.

Im Bereich der Automatisierungs- und Industrietechnik haben sich in den vergangenen Jahren bereits IP-basierte Netztechnologien entwickelt, die auf erhöhte Zuverlässigkeits- und Echtzeitanforderungen optimiert sind. Die Erfahrungen und technischen Grundlagen dieser zumeist auf Ethernet basierenden Echtzeitvarianten stellen den Ausgangspunkt für die Evaluierung potenzieller Lösungen für den Automobilbereich dar. Auf Basis der verschiedenen Systemansätze und automobilspezifischen Anforderungen werden unterschiedliche Physical Layer und Netztopologien bezüglich ihrer Eigenschaften für das Einsatzgebiet untersucht.

Durch die schnelle Entwicklung im Multimediabereich sind dort bereits grundlegende Technologien und Protokolle verfügbar, um

IPV4 ODER IPV6?

Internetanbieter können bald nicht mehr allen Kunden eine eindeutige IPv4-Adresse anbieten – der Adressraum ist fast aufgebraucht. IPv6 wird in Zukunft also eine größere Rolle spielen als bisher. Gleichzeitig existieren eine Reihe von Anwendungen im und um das Fahrzeug auf der Basis von IPv4, die nicht sofort umgestellt werden können. Das Projekt SEIS untersucht daher gemischte Szenarien, die sowohl IPv4- als auch IPv6-Geräte zulassen.



2 Teilprojekte des SEIS-Projekts

Multimediadaten in Echtzeit über IP zu übertragen. Dies sind beispielsweise die Protokolle RTP und RTSP für Streaming, PTP für die Synchronisation, sowie diverse QoS-Standards auf verschiedenen Schichten. Die „Audio Video Bridging Working Group“ (AVB) der IEEE standardisiert momentan spezielle Erweiterungen des Ethernet-Standards, um in Ethernet und IP-basierten Netzen die Qualität von Echtzeit-Medienströmen schon auf der Sicherungsschicht garantieren zu können.

Um zu einer einheitlichen IP-basierten Kommunikation im Auto zu kommen, sind auch auf den höheren Schichten einige technische Herausforderungen zu lösen. Neben dem Internet Protokoll im engeren Sinne (IPv4 beziehungsweise IPv6, siehe Info-Kasten) gehören zur Internet-Protokollfamilie eine Reihe von Schwesterprotokollen, zum Beispiel für Routing oder Ressourcensteuerung. Steuergeräte im Fahrzeug werden nicht in der Lage sein, die gesamte Vielfalt der Internetprotokolle abzubilden. Daher wird sich die technische Lösung für diese Geräte auf ein Mindestmaß beschränken müssen.

4 TEILPROJEKT SYSTEMSOFTWARE / MIDDLEWARE

Als Middleware wird Systemsoftware bezeichnet, die verteilten Software-Anwendungen eine Basisfunktionalität zur Verfügung stellt. Klassische Aufgaben von Middleware sind beispielsweise die Bereitstellung sowohl einer lokalen als auch geräteübergreifenden Kommunikationsinfrastruktur auf Anwendungsebene (verteilte Funktionsaufrufe), die Verwaltung von verteilten Ressourcen im System, sowie die Bereitstellung von systemweiten Diensten (beispielsweise Adressierungsdienste).

Im Fahrzeug ist es heute üblich, dass die dort eingesetzte Vernetzungstechnologie je nach Anwendungsdomäne auch eine Middleware-Lösung vorgibt. Aufbauend auf dem Most-Bus gibt es beispielsweise die Most-NetServices. Für die lokale Interprozesskommunikation wird oft der „virtuelle Most-Bus“ verwendet. In anderen Domänen werden Daten auf der Grundlage von einfachen Signalen übertragen.

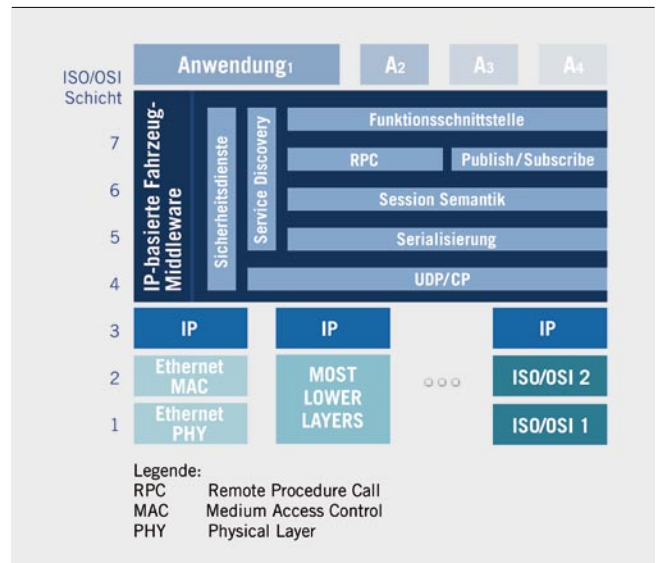
Diese existierenden Lösungen sind nicht unmittelbar kompatibel, sodass komplexe Gateways eingesetzt werden müssen, wenn eine domänenübergreifende Kommunikation benötigt wird. Wenn

beispielsweise in einem Fahrzeug ein an Flexray angeschlossenes Gerät eine Aktion auf Anforderung eines Most-Geräts durchführen soll, zum Beispiel eine Parametereinstellung, passiert folgendes: Das Most-Gerät schickt einen Funktionsaufruf an einen Most-Funktionsblock im zentralen Gateway. Der schickt ein entsprechendes Flexray-Signal an das ausführende Gerät. Bei dieser Umsetzung werden eventuell Parameter umcodiert, eine Most-Nachricht in mehrere Flexray-Signale übersetzt etc. Sendet das Flexray-Gerät eine Antwort zurück, wird diese wiederum vom Gateway empfangen, umcodiert und in entsprechender Darstellung auf Most zurückgesendet. Aus einer einfachen Interaktion zwischen zwei Geräten wird in der Realisierung im Fahrzeug eine komplexe Interaktion von drei Geräten, wobei auch das Gateway als Vermittler Anwendungswissen benötigt und bei Änderungen der Anwendung entsprechend angepasst werden muss.

Der Einsatz des Internet Protokolls kann diese Situation vereinfachen. Eine durchgängige, skalierbare Middleware-Lösung ermöglicht eine direkte domänenübergreifende Kommunikation, ③. Im obigen Beispiel könnten die beiden Geräte direkt über die gleiche IP-Middleware kommunizieren, ohne dass ein Gateway notwendig wäre. Selbst wenn die Geräte mit verschiedenen Netztechnologien angebunden sind, ist als Vermittler nur ein IP-Router nötig, der keinerlei Anwendungswissen braucht.

Konkretes Ziel des Teilprojekts Systemsoftware ist die Entwicklung einer IP-basierten Fahrzeug-Middleware, die domänenübergreifend funktioniert. Für unterschiedliche Geräteklassen sind verschieden große Ausprägungen der Middleware geplant – wichtig ist, dass auch ein kleineres Gerät direkt mit einem mächtigeren kommunizieren kann.

Geplant ist auch die Teilnahme in entsprechenden Konsortien (beispielsweise Autosar und GENIVI), um die Ergebnisse frühzeitig dort einzubringen und damit eine herstellerübergreifende Standardisierung voranzutreiben.



③ IP-basierte Fahrzeug-Middleware

5 TEILPROJEKT SICHERHEIT

Ziel des Teilprojekts Sicherheit ist es, das Gesamtsystem sowohl gegen mutwillige Angriffe, als auch gegen Überlastung und Fehler robust und datensichernd auszulegen. Um die ordnungsgemäße Funktion zu jedem Zeitpunkt sicherzustellen, konzentrieren sich die Arbeiten auf die Angriffssicherheit von Fahrzeugen.

Es muss nachgewiesen werden, dass sich alle Anforderungen an die Kommunikation innerhalb von Fahrzeugen auch mittels IP realisieren lassen, ohne Einbußen an der Zuverlässigkeit einzelner Bordsysteme oder der Betriebssicherheit eines Fahrzeugs. Dazu



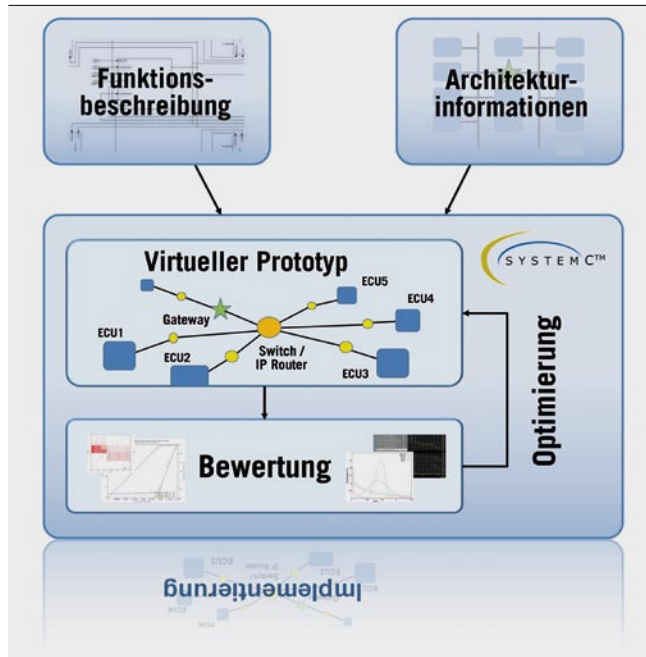


International Exhibition
& Conference for
POWER ELECTRONICS
INTELLIGENT MOTION
POWER QUALITY
4 – 6 May 2010
 Exhibition Centre Nuremberg

Leistungsstark

Hier sind Sie richtig!

Mesago PCIM GmbH – 0711 61946-56 – pcim@mesago.com



4 Bewertung und Optimierung mittels virtueller Prototypisierung

zählt, dass Echtzeitfähigkeit, Robustheit und Fehlertoleranz sowie QoS Anforderungen mit den Sicherheitsanforderungen in Einklang gebracht werden.

IP-basierte Kommunikation im Fahrzeug hat neben der Robustheit auch Sicherheitsziele wie Authentizität, Integrität, Vertraulichkeit und Datenschutz auf geeigneter Ebene zu adressieren. Hierzu sind bedarfsorientierte Sicherheitsfunktionen [2] wie Authentisierung, Autorisierung von Zugriffen und Funktionsaufrufen, Schutz gegen Überlast bei Angriffen und Querschnittsfunktionen wie Schlüsselmanagement zu analysieren und zu entwickeln, um die Einzelfunktionen in einer Systemarchitektur entsprechend der verschiedenen Betriebszustände abzusichern und gegen Angriffe zu schützen.

Eine Integration von IP in die Bordnetzarchitektur stellt durch die weite Verbreitung dieser Technologie ein erhöhtes Gefährdungspotenzial dar. Zunächst werden daher die mit IP vernetzten, eingebetteten Steuergeräte in einem Domänenmodell abgebildet, um den Schutzbedarf der Teilsysteme wiederzugeben und hierauf das Sicherheitskonzept des Gesamtsystems aufzubauen. Des Weiteren wird dieses Modell den Schutzanforderungen und den zu erwartenden Sicherheitsproblemen Rechnung tragen und somit eine Referenz für die Kommunikationsinfrastruktur im Fahrzeug bilden.

Definierte Sicherheitsziele wie Authentizität, Integrität und Vertraulichkeit müssen für die angestrebte homogene Kommunikationsinfrastruktur nach jeweiliger Notwendigkeit sichergestellt werden. In IP-basierten Netzen existiert eine Vielzahl von Verfahren, diese Ziele zu erreichen. Lösungen für den Schutz vor Angriffen und Missbrauch sind aus dem IT-Umfeld bekannt. Um die Besonderheiten des automobilen Bedarfs abzudecken, müssen diese möglicherweise angepasst oder erweitert werden.

Neben den Steuergeräten haben auch Anwendungen und gemeinsam genutzte Funktionen einen dedizierten Schutzbedarf

bei der Abwicklung ihrer Interaktionen. Sicherheitsvorfälle sind zu erfassen und Grenzen von Fehlererkennung und Fehlerkorrektur, Robustheit und Zuverlässigkeit einzuhalten. Zusätzlich soll untersucht werden, wie die Software von Steuergeräten sicher ausgetauscht werden kann und wie diese gegen Manipulation zu schützen ist.

Wenn mit Entitäten außerhalb des Fahrzeugs kommuniziert wird, ergeben sich Fragen nach der Authentizität des Kommunikationspartners und den geeigneten Transportmechanismen. Die Umschaltung zwischen verschiedenen physikalischen Transportmedien soll für die Kommunikationspartner transparent erfolgen, so dass bestehende Verbindungen nicht unterbrochen werden. Anwendungsspezifisch muss das benötigte Maß an Authentizität, Integrität und Vertraulichkeit von übermittelten Daten festgelegt und so in technische Konzepte umgesetzt werden, dass Beeinflussung und Gefährdungen für Fahrer, Fahrzeug und die direkte Fahrzeugumwelt vermieden werden.

Dazu werden Angriffe betrachtet, die ungewünschten Einfluss auf Systemfunktionen oder das System haben können. Die erarbeiteten Anforderungen der veränderten Bedrohungslage bei einer direkten Verbindung des Fahrzeugs zum Internet werden aufgegriffen und in entsprechende Schutzmechanismen überführt.

Des Weiteren müssen Maßnahmen identifiziert werden, um das IT Sicherheitsniveau eines Neufahrzeugs über dessen Gesamtlebenszeit aufrecht zu erhalten. Im Gegensatz zu Rechensystemen in der Büro- und „Consumer“-Welt, die regelmäßig durch Updates mit neuen Softwarepatches und Virensignaturen versorgt werden können, ist das Security Management für in Fahrzeuge eingebettete Steuergeräte ungleich schwieriger. Einerseits sind Fahrzeuge nicht ständig erreichbar, andererseits darf das Service Management nur durch vom Hersteller legitimierte und autorisierte Software erfolgen.

6 TEILPROJEKT BEWERTUNG UND OPTIMIERUNG

Wie das Beispiel Flexray in der Vergangenheit gezeigt hat, hat die Umstellung auf eine neue Kommunikationstechnologie gravierenden Einfluss auf den Entwurfsprozess der gesamten E/E-Architektur eines Fahrzeugs. Die Herausforderungen im Kontext IP-basierter Technologien liegen in der ganzheitlichen Modellierung von verschiedenen Topologien mit speziellen Koppellementen, der steuergeräteinternen Communication-Controller sowie der Funktionsschnittstellen. Vor dem Hintergrund harter Echtzeitanforderungen und Kostenbeschränkungen sollen Qualitätsmerkmale wie Echtzeitfähigkeit, Energieeffizienz und Zuverlässigkeit analysiert und die gesamte E/E-Architektur hinsichtlich dieser Kriterien optimiert ausgelegt werden.

Ziel ist eine Methodik zur frühzeitigen Bewertung von IP-basierten E/E-Architekturvarianten. Ein möglicher Ansatz basiert auf einer Kombination von formalen und ausführbaren Spezifikationen, 4. Hierdurch können die Einflüsse von Architekturentscheidungen bereits in den frühen Entwurfsphasen sowohl formal als auch simulativ quantifiziert und berücksichtigt werden. Der auf der Entwurfssprache SystemC [3] basierende Ansatz erlaubt die virtuelle Integration unterschiedlicher Technologien, Koppellemente, Steuergeräte sowie der Funktionsverteilung in einem ausführbaren Modell der E/E-Architektur. Durch die virtuelle Prototypisierung muss nicht mehr gewartet werden, bis alle Komponenten

ten verfügbar sind. Zukünftige E/E-Architekturen werden stattdessen als virtueller Prototyp am Rechner inklusive Zeitverhalten, Energieverbrauch etc. simuliert. Hierdurch werden Entwurfsrisiken minimiert [4], da notwendige Korrekturen und Optimierungsmaßnahmen frühzeitig erkannt und eingebracht werden können.

Ein bisher ungenutztes Potenzial der virtuellen Prototypisierung liegt in der Erforschung intelligenter Energiemanagementstrategien. Eine Umstellung auf IP-basierte Technologien mit ihren flexiblen Vernetzungstopologien bietet neue Möglichkeiten, den Energieverbrauch und somit den CO₂-Ausstoß im Betrieb zu reduzieren. Im Projekt SEIS werden insbesondere das individuelle Herunter- beziehungsweise Hochfahren von Kommunikationsclustern im Betrieb oder die Ausnutzung verschiedener Power-Modi der Schnittstellen untersucht. Die Effizienz dieser Maßnahmen hängt maßgeblich von der gewählten Funktionsverteilung ab. Virtuelle Prototypen sind hierbei der Schlüssel zu einer energieoptimierten Auslegung der IP-basierten E/E-Architektur.

7 DIE DEMONSTRATOREN

Alle am SEIS-Projekt beteiligten OEMs planen den Aufbau jeweils eines Fahrzeugs, in dem die Vorteile von IP-basierter Kommunikation erlebbar sein werden. Die Grundlage hierfür werden existierende Fahrzeugkomponenten sein, die um die entsprechende IP- bzw. Sicherheitsfunktionalität erweitert werden. Außerdem wird es Technologiedemonstratoren geben, um Schlüsselanforderungen in Messaufbauten absichern zu können. Die Demonstratoren sollen Eigenschaften nachweise, die folgend beschrieben werden:

- : Echtzeiteigenschaften, wie garantierte Latenzzeiten für zum Beispiel Fahrerassistenz-, Steuer- und Sensor-Daten
- : garantierte Bandbreite für Audio und Video, garantierte Zustellung von Informationen
- : robuste Koexistenz von Real Time- und Best Effort-Verkehr auf derselben Netztechnologie
- : Plug-and-Play-Kommunikation verschiedenster Geräte im Fahrzeug
- : sichere Interaktion mit gekoppelten Geräten und mit Funktionen, die über das Internet verbunden sind
- : Authentifizierung und Autorisierung von Funktionen
- : Schutz vor unterschiedlichen Angriffen und Überlastsituationen.

8 FAZIT

Das Projekt SEIS wird die Komplexität der Elektronikarchitektur reduzieren, indem es die Grundlagen für IP als gemeinsame Vernetzungstechnologie für Steuergeräte im Kraftfahrzeug legt. In den Teilprojekten des SEIS-Projekts wird der gesamte Kommunikationsstack von den Technologien bis zu den Anwendungen abgedeckt; der Schwerpunkt des Projekts liegt auf einer durchgängigen Sicherheitslösung für die IP-vernetzten Systeme.

Die Ergebnisse aus diesem Projekt schaffen wichtige Grundlagen für alle Bereiche der Datenvernetzung im Kraftfahrzeug. Sie erlauben es – trotz wachsender Komplexität der Bordelektronik – auch zukünftig neue, innovative Lösungen entwickeln zu können, die einen weiterhin hohen Standard bei Sicherheit und Zuverlässigkeit gewährleisten.

Durch die Zusammensetzung des Konsortiums mit den meisten deutschen OEMs, wichtigen Zulieferern, Technologiepartnern und

namhaften Forschungseinrichtungen ist zu erwarten, dass die im Projekt erarbeiteten Lösungen breite Akzeptanz in der Industrie und Forschung haben werden.

LITERATURHINWEISE

- [1] <http://www.eenova.de/projekte/seis/>
- [2] C. Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 6. Auflage, Oldenbourg, 2009
- [3] <http://www.systemc.org>
- [4] C. Haubelt, J. Teich und R. Dorsch. Entdecke die Möglichkeiten. In Design&Elektronik (8):22-27, 2008



DOWNLOAD DES BEITRAGS

www.ATZonline.de



READ THE ENGLISH E-MAGAZINE

order your test issue now: SpringerAutomotive@abo-service.info

Embedded Tester

Die Testumgebung für TargetLink®

Sparen Sie bis zu 50% Testaufwand!

- /// Automatische Testfallgenerierung
- /// Testausführung MiL, SiL und PiL
- /// Automatisierter Back-to-Back Test
- /// Automatische Code-Verifikation
- /// Debugging-Unterstützung
- /// Test- und Coverage-Berichte
- /// ISO/DIS 26262 Testkriterien (ASIL A-D)
- /// Automatisierter Test-Workflow
- /// Enge Integration mit TargetLink®

Besuchen Sie uns auf der
Embedded World 2010
2. - 4. März 2010 in Nürnberg
auf dem dSPACE Stand 125 in Halle 10

www.btc-es.de

Just in Case!

BTC
Embedded Systems