

RealTimes

J 2017/2018

www.etas.com



コネクテッドビークルの免疫システム | Page 08

ファンクションの迷宮を抜ける新たな道筋 | Page 24

RDE - 車両の排ガスを実際の運転条件下で測定 | Page 30



Christopher White
Executive Vice President Sales

Friedhelm Pickhard
President

Bernd Hergert
Executive Vice President
Operations

読者の皆様へ

私たちは今、自動車エレクトロニクス開発にとって非常にエキサイティングな時代を経験しています。クラウドを経由したインテリジェントな（半）自動運転技術を追求める機運はますます高まっています。効率、代替パワートレインシステム、コネクテッドモビリティ、IoT（モノのインターネット）接続 — これらはすべて重要な役割を担うテーマです。しかし、説得力のあるセキュリティソリューションと包括的なセキュリティコンセプトがなければ、自動運転の実現は不可能です。

デジタル化が進む時代には、システムのセキュリティに特に注意を払う必要があります。コネクテッドピークルシステムのデータや機能への不正アクセスに対する防御を求める声は高まるばかりです。ライフサイクル全体にわたって継続して修正し適応させることは、サイバーセキュリティにとって極めて重要な要素となります。コネクテッドピークルには、新しい攻撃シナリオにも直ちに反応することのできる学習型の車両防御システムが必要です。自動車分野において、弊社は子会社の ESCRYPT とともに専門性の高いセキュリティソリューションを提供してきました。将来的には増大するセキュリティ要件に対応できる、IoT 環境の統合型サイバーセキュリティソリューションの製品ラインを築き上げることを目指しています。

今号の RealTimes では、テクノロジーとエレクトロニクスに情熱を注ぐ ETAS と ESCRYPT が、その時々課題に取り組み、そして克服していく様子をご紹介します。新しい ETAS ソリューションに関する記事では、弊社の多岐にわたる製品やサービスを活用する可能性についてご説明しています。たとえば、実路走行排気（Real Driving Emissions, RDE）のテストドライブを高い再現性で制御して実行できる弊社のソフトウェアソリューション、INCA-RDE についてご案内しています。別の記事では、ファンクションのモデルベース開発を支援する新しい SCODE 製品ファミリをクローズアップしています。また、弊社のソリューションを導入したお客様の成功事例では、その効果を証明しています。さらに、弊社が各種研究機関と密接な協力関係を築いていることもご理解いただけるでしょう。この関係は、「ノウハウの水準を高く保ち、新しい技術要件にソリューションを適応させ最適化し続ける」という弊社の基本戦略に基づいています。

今号の示唆に富む記事をお楽しみいただけたら幸いです。日頃より弊社の業務へのご協力とご理解に感謝申し上げます。弊社は将来を見通したソリューションの共同開発を通じて、素晴らしい未来を皆様と共に歩んでいけることを楽しみにしております。

Friedhelm Pickhard

Bernd Hergert

Christopher White

Contents

- 05 **イーサネットのセキュリティ**
プロダクションキーサーバーによるセキュアな鍵管理
- 08 **コネクテッドビークルの免疫システム**
侵入検知・防御システム (IDPS)
- 12 **仮想車両で組み込みセキュリティのテストを実施**
XiL テスト環境を利用してハッキングを詳細にシミュレート
- 14 **始めから終わりまで徹底的にテスト**
車のライフサイクル全体にわたるセキュリティテスト
- 15 **大きな一歩**
ETAS ASCET-DEVELOPER 7 — 組み込みソフトウェアの安全性向上を手軽に実現
- 16 **安全性とセキュリティ対策のコーディング**
ESDL を用いた、よりセキュアなソフトウェアの実装
- 19 **量産車に仮想ECU を搭載？**
ETAS Lightweight Hypervisor による柔軟性、高効率性、セキュリティ対策の実現
- 22 **ECU ソフトウェアの継続的納入**
電動化を促進するアジャイルソフトウェア開発
- 24 **ファンクションの迷宮を抜ける新たな道筋**
- 26 **車両システムのシミュレーションと仮想化**
分散化ECU ファンクションの開発とテストをETAS COSYM で
- 28 **ロバストな運転支援システム**
反復検証のための戦略
- 30 **ETAS INCA-RDE**
車両の排ガスを実際の運転条件下で測定
- 33 **ガソリンエンジンの最適化**
Hyundai におけるモデルベース適合
- 35 **ETASの学生支援**
- 40 **製品情報**
- 42 **写真で振り返るETAS の1年**
- 44 **会社情報**
- 46 **ETAS Automotive India の10年**
ETAS インド法人がお客様と一緒に10周年を祝いました
- 48 **お客様の身近に**
ETAS のカスタマーサポート
- 50 **パートナーシップと協業**
- 51 **Locations and Imprint**

イーサネットのセキュリティ

Ethernet Security



執筆者

Norbert Fabritius

Ramona Jung

ESCRYPT GmbH

セキュリティエンジニア

Dr. Jan Holle

ESCRYPT GmbH

セキュリティエンジニア&

プロダクトマネージャ

ESCRYPT は ETAS GmbH の 100% 子会社です。組み込みシステム向けのセキュリティソリューションを提供しています。

プロダクションキーサーバーによるセキュアな鍵管理

イーサネットは、データセンターやコンシューマーセクターで広く使用される IT 規格として 40 年以上にわたって定着しており、今や自動車業界も席巻しています。E/E アーキテクチャは当初、クロスドメイン通信を行わないシステムに適用されていましたが、今日ではドメインの境界を越えて展開されるようになってきています。その結果、セキュリティや安全性、また確実な応答挙動時間をめぐってさまざまな問題が持ち上がり、実用的なイーサネットソリューションが求められています。

さまざまな安全関連プロトコル
(緑色の部分)

車載システムにおいては、データ転送の高速化が急ピッチで進んでいます。それに対応するため、CAN や FlexRay などの従来のバスシステムをサポートし、その安全を守る新しいイーサネットが業界内で新たに登場しています。インフォテインメント分野で生まれたイーサネットの技術は、今日ではクロスドメインの車載システムにも使用されるようになりました。

データバスがセキュアに、単独または他のデータバスとの通信で確実に機能するためには、十分に考え抜かれたロバストなソリューションが必要です。このソリューションは、従来のバスとのシームレスなデータ交換だけでなく、イーサネットコンポーネント間の通信にも対応できるものでなければなりません。必要に応じて、イーサネット (Ethernet) の規格を車載システムの具体的な要件に適合させることが非常に重要です。従来の IT ソリューションをそのままに、または少し修正するだけで使用できる場合もありますが、新しいソリューションを開発しなければならない場合もあります。その判断は、ビデオ信号などのような大量のデータを取り扱う際に、最大限のセキュリティや安全性、また確実な応答挙動時間を実現するために、どのような方法を選択するかによって決まります。

典型的 IT の諸問題とソリューション

イーサネットの分散型構造により、冗長化または動的ネットワークバスを用いることで、単一障害点となる集中管理のエンティティの使用を回避することができます。ただし、この分散型構造そのものにも疑問が生じます。たとえば、イーサネットネットワークのすべてのメンバーが同じ特権を持っている場合、あるメンバーがネットワークに不正にアクセスし

アプリケーション	アプリケーションプロトコル		Audio Video Bridging (AVB)
プレゼンテーション			
セッション		SecOC	
トランスポート	TCP/UDP	TLS/DTLS	
ネットワーク	IP	IPsec	
データリンク	Ethernet MAC	MACsec	VLAN
物理	100(0)BASE-T1		

ようとしているのを検知してそれを禁止するには、どうすればよいでしょうか。また、ネットワークマニピュレーションを識別して阻止するには、どうすればよいでしょうか。

この問題の対応として、たとえば仮想ネットワーク (VLAN) を使用してネットワークトラフィックの分配を行うようなソリューションの確立があります。本来、ネットワークポートは各種 VLAN のスイッチに割り当てられるものでしたが、今ではイーサネットフレームとポートに依存しない VLAN をマーク (「タグ」) によって関連付けることもできます。このタグ付けは IEEE 802.1Q 規格に規定されています。しかし、ネットワークトラフィックを論理的に分けるだけでは、不審なデバイスによるネットワークへの接続を防ぐことはできません。また、マニピュレーションやスパイ行為からも、条件付きでしかネットワークを保護することができません。これらの防御を完全に行うためには、暗号化認証または暗号化が必要です。この問題に対応する、昔ながらの IT ソリューションも存在します。初期のソリューションでは、データフォーマットや Transport Layer Security (TLS) などの規格を通じて上位のプロトコルレイヤに注目しましたが、その後のソリューションでは、さら

に下位のレイヤに関するセキュリティメカニズムも追加されました。これには、IPsec による IP パケットの暗号化 (レイヤ 3) や、MACsec (IEEE 802.1AE) によるイーサネットフレームの暗号化 (レイヤ 2) が含まれます。これらのソリューションもまた業界標準により規定されています。

さらに、以下のようなセキュリティコンポーネントも利用できます。従来型のファイアウォールは、フィルタールールに基づいて、ネットワークまたはエンドポイントに出入りするパケットの許可をコントロールします。現代のバリエーションはさらに、ディープパケットインスペクション (DPI) でトラフィック内のパケットのペイロードまでを分析して検査することができます。不正侵入検知システム (IDS) と不正侵入防御システム (IPS) はこれを基礎に構築されるもので、これにより管理者もコントロールオプションを使用できるようになります。

現代の車載ネットワークのセキュリティ要件

現代の車両のネットワークアーキテクチャと従来の IT で使用されていたネットワークアーキテクチャには、多くの類似点があります。しかし、技術基準や防御目標は両者の間で大きく異なります。

車両においては、搭乗者の安全と所有資産が最優先されるため、システムの可用性とネットワークトラフィックの信頼性が重要視されます。さらに、「ネットワークコンポーネントは事実上遅延なく決定論的手法でなければならない」という、車両運転におけるリアルタイムの重要性が関与します。

これらの要件は、データの packets 通信時間の保証を必要としない、パケットベースのネットワークがベストエフォート型のイーサネットの性質に明らかに反しています。また、車載 ECU の計算能力は限られているため、安全目標を達成してリアルタイム要件を実現するのは困難です。

このような理由から、定評のあるセキュリティ技術に修正を加えて車載ネットワークに実装するという事はよくあります。たとえば、ネットワークのフェイルセーフ特性を強化するために VLAN を使用することがあります。この場合、ネットワークを、それぞれ異なる防御が必要な複数の仮想ゾーンに分割し、それらの仮想ゾーンによって安全関連コンポーネントのネットワークトラフィックをリアルタイムに識別できるようにします。そうすれば、特定のトラフィックを必要に応じて他より優先的に扱ったり、他と分離したりすることもできます。優先度の高い VLAN 間の通信に対して優先的に帯域制限を行うことにより、サービス妨害 (DoS) 攻撃や故障コンポーネントで大量の packets がネットワークに送り込まれても、スイッチ一つで阻止することができます。

ファイアウォールが、それより強力な IDS/IPS システムを使用することで、互いに異なる防御要件を持つ、隣接する IP ネットワーク同士をより確実に分離し、より正確に監視することが可能になります。それに対し、従来の車載バスシステムは、ブロードキャストメディアであるため、論理的に (つまり、追加の物理バスをインストールしないで) 分離することはできません。

既存と新規の セキュリティソリューション

かつて TLS IT セキュリティプロトコルの使用には注意が必要でした。なぜなら、このプロトコルは車両のリアルタイム要件と相反する恐れがあったため、時間を重視しないバックエンドシステムやテスト装置との通信でしか使用を検討することができなかったからです。しかし、TLS 1.3 仕様では大幅な革新が見られました。接続の確立方法が最適化されたため (ゼロ RTT ハンドシェイク)、TLS で保護されたデータをハンドシェイク中の最初の packets に収容できるようになりました。このため、TLS を使用してもらウンドトリップタイム (RTT) が無駄にかかることはなくなりました。事前共有鍵 (TLS-PSK) を使用することで非対称処理が不要になるので、TLS のオーバーヘッドコストも劇的に低減することが可能になります。ただし、当面は、TLS のセキュリティ保証の弱点に関する可能性を念入りに検査することに重点が置かれています。

車両におけるリアルタイム要件は、非対称処理に基づく暗号署名を使用する場合に障害になります。データ packets の信頼性を保護するために、2014 年に AUTOSAR 4.2 の一環として Secure On-Board Communication (SecOC) モジュール仕様が発表されました。SecOC 仕様は非常に柔軟性のある内容なので、Ethernet/IP ベースのトラフィックにも適しています。

同様に、本来スピード重視のビデオデータの送信用に開発された Audio Video Bridging (AVB) のような、各種の Time-Sensitive Networking (TSN) 規格も利用可能です。これらの規格は、イーサネットの通信でも適用されるもので、ネットワークリソースの予約、時刻信号の同期化、およびデータストリームの優先順位付けを管理する独自のメカニズムを規定しています。しかも、AVB は従来型のバスデータの伝送も可能です。この規格では、基礎的なテクノロジーとしてのイーサネットを拒絶することなく、リ

アルタイム仕様を伴う環境の要件を考慮することができます。AVB トランスポートプロトコルの最新バージョン (2016 年末期現在) は、送信されるペイロードデータの暗号化にも、比較的低いハードウェア要件で必要に応じて対応することができます。

車両におけるイーサネットの セキュリティ 開発と統合

イーサネットベースのソリューションを車載ネットワークに統合する動きは本格的に進んでいます。イーサネットの規格を使用すれば、将来の車両に期待される各種機能を実装することができます。しかも、この進歩は車両のセキュリティ要件に反するものでは決してありません。セキュリティの専門家による綿密なサポートとお客様に合ったセキュリティソリューションにより、セキュアなイーサネットアーキテクチャの実装を、きわめて複雑であるにもかかわらず成功させることが可能です。これを実現するために、ESCRYPT のイーサネットセキュリティと自動車の分野における長年の経験を活用することができます。このノウハウを生かし、実行可能なセキュリティ概念の構築と分析から、自動車業界のニーズに合わせてカスタマイズしたソフトウェアとハードウェアのソリューションを弊社の幅広い製品への実装まで、イーサネット統合の全段階にわたってお客様をサポートいたします。

イーサネット規格は、インテリジェントなセキュリティソリューションやセキュリティ製品に保護されながら、40 年以上にもわたるサクセスストーリーにエキサイティングな次章が書き加えられています。そして、それらの新たな章は、自動車業界において、かつてないほどの脚光を浴びようになるはずで

Immune System for the Connected Vehicle

コネクテッドビークルの 免疫システム



執筆者

Dr. Jan Holle
ESCRYPT GmbH

セキュリティエンジニア&
プロダクトマネージャ

ESCRYPTはETAS GmbHの100%子会社です。組み込みシステム向けのセキュリティソリューションを提供しています。

侵入検知・防御システム (IDPS: Intrusion detection and prevention system)

安全性と快適性が高まり、サービスが最適化され、車の運転をより楽しめる。コネクテッドビークルには多くの長所があります。しかし、「モノのインターネット (IoT)」に組み込まれることにはリスクも伴います。IoT ではサイバー攻撃の危険が増大し、悪用できそうな新たな脆弱性を攻撃者たちが絶えず探し求めています。そのため、コネクテッドビークルには、未知のパターンの攻撃さえも検知して、新しい攻撃パターンをネットワーク上の他のコネクテッドビークルに迅速に伝えることのできる、学習型の防御システムが必要です。

車両が一度お客様に所有されると、メーカーはその車両システムに時折アクセスする程度になります。しかし、それでも購入者は自分の車両がいつも保護されていることを当然のこととして期待します。車両が続々とコネクテッド化される中で、新たな問題も持ち上がっています。IoT に組み込まれると、確かにメーカーが車両にアクセスできる可能性は高まることになりませんが、それと同時に車両が不正アクセスや悪意のあるサイバー攻撃を受けるリスクも高まっています。もはや機能安全だけでは不十分です。世界中の道路を何億台ものコネクテッドビークルが走行することになるのであれば、メーカーは包括的な自動車 IT セキュリティも保証しなければなりません。これに加えて、私たちは今後の自動運転の動向も考慮しなければならないため、IT システムの安全性とセキュリティに関する要求がますます増えることとなります。

ライフサイクル全体にわたる包括的防御
要求されるセキュリティレベルを実現する前提として、十分に考え抜かれた方策が効果的に実施されなければなりません。自動車のセキュリティは後付けできません。少なくとも莫大なコストをかけなければ不可能です。それに代わる方策として、開発の開始から安全性とセキュリティを考慮していくという全体論的な戦略が必要になります。このソリューションには、信頼できる防御策など、組

み込みソフトウェアの開発段階で標準化されるプロセスも含まれます。ハードウェアセキュリティモジュールやセキュアハードウェアエクステンションを含む、ハードウェアセキュリティアドオンを使用する現代のチップアーキテクチャは、安全関連のシステムドメインを不正アクセスから物理的に保護します。これらのセキュリティコアの周りにはさらに、ECU ファームウェアのマニピュレーションを認識するセキュアブート機能や、すべての通信を保護するための保護ネットワークゲートウェイまたは暗号ソリューションなどの方策が必要です。同じく重要なのは、セキュリティエリアへのアクセスを制限することや、暗号鍵およびロック解除コードのアクセス権を責任能力のある数名の個人だけに与えること、開発・製造段階における組織的な防御策です。

上述の方策は、偶発的なエラーの可能性を下げ、ハッカーによる車載システム侵入の試みを阻止します。しかし、これらの方策だけでは、お客様の所有物となった車両のコネクテッドシステムの防御をどのようにして保証するかという問題の解決にはなりません。ライフサイクルの中段階にもなると、メーカーは限られた機会しか車両にアクセスすることができません。理屈の上では、今後 10 年以上にわたる攻撃に対処できるように、メーカーが開発段階のうちに車両システムに対策を施しておくことが必要ということになります。しかし、10 年前の情報技

術の状況を振り返ってみても、そのようなことは到底不可能であることがわかるはずで

課題：未知の危険に対する防御

論理的結論としては、車両がお客様に所有されていても、そのシステムを確実に防御するために、IT セキュリティ対策は動的でしかも継続的なものでなければなりません。ただし、機能安全の境界条件は主として自然法則や統計的予測に基づいていて、車両の使用段階でもそのまま適用されることになりませんが、IT セキュリティの仮定と境界条件は不安定で変わりやすいものです。攻撃者はシステムの新たなウィークポイントを絶えず探し求めています。メーカーはこれらのウィークポイントの存在にそもそも気付いていない場合がほとんどです。一方、セキュリティ専門家も、今後何年もの間に出現する可能性のあるすべての攻撃戦略を予知することはできません。既存の IT も、未知のパターンを用いた攻撃から IT インフラストラクチャを防御するという難題に直面しています。この場合も、攻撃者は完全な防御を実現するように考え抜かれたセキュリティメカニズムを回避しようとします。この分野では次第に、「防御」とはすなわち「インテリジェントな侵入検知・防御システム (IDPS) を整備すること」を意味するようになりつつあります。さらによく注目すると、IDPS は、コネクテッドビークルの保護にも最適なシステムであることがわかります。

IDPS による予防措置

IDPS テクノロジーならではの強みは、車両の接続性を使用することによって新しい攻撃シナリオに素早く反応することができ、さらにその防御戦略をすぐに車両フリート全体に伝えることができることです。これにより、攻撃に対して動的に反応する一種の免疫システムが構築され、その免疫システムの下では新たな攻撃が発見されるたびにフリートの防御力が強化されていきます。

ESCRYPT の IDPS の中核となっているのは、ECU やゲートウェイを監視して車載ネットワークの電気通信全体を絶えず分析し続ける特別なセキュリティソフトウェアです。異常が発生すると、このソフトウェアはそれを記録し、さらに、深刻な脅威が存在する場合は防御策を推進します。検知された攻撃パターンが既

知のものである場合は、ファイアウォールメカニズムが各種データベース間の通信をブロックします。これはすでに日常的な流れであり、IDPS 全体と同様に、将来のイーサネットネットワークだけでなく、今日の主流である CAN のネットワークでも使用することができます。

しかし、IDPS テクノロジーの真価は、未知のパターンと攻撃戦略を認識して撃退できることにあります。これを行うために、IDPS はルールセット（ブラックリストとホワイトリスト）を複数個保有して、その内容は絶えず更新されています。このアプローチの強みの1つとして、異常や未知の攻撃の手がかりは“CycurlDS”という攻撃認識ソフトウェアによって検知されますが、このソフトウェアは、異常に関する情報を後で

見直せるように車両に保存しておくことができます。そして、さらに効果的なのは、すべての異常に関する情報をクラウドベースのイベントデータベースに自動送信する機能です。イベントデータベースには、同じメーカーのすべてのコネクテッドビークルから送信されたすべての異常に関する情報を、既知の攻撃者の履歴情報と一緒に格納するので、分析時にはそれらを効果的に比較することができます。

フリート全体に対する動的防御戦略の構築

データの分析から、OEM はハッカーがどのような戦略を遂行しているかのウィークポイントを標的にしているか、そして特定の領域に攻撃が集中しているかどうかという点について、常に最新の



包括的概観情報を受け取ります。この包括的なイベントデータベースをバックエンドで評価するために、動的防御システムの次の段階として、ビッグデータを自動分析する CycurGUARD ソフトウェアソリューションが稼働します。このソフトウェアは攻撃パターンを分析して事前分類処理を実行します。それに基づいて、サイバーディフェンスセンターのセキュリティアナリストと犯罪科学スペシャリストが、対抗措置が必要かどうか、および必要な場合はどの対抗措置を開始するべきかを決定します。その措置としては、ファイアウォールの調整や、CycurIDS ルールセットの更新、また影響を受ける ECU のソフトウェアに内在する脆弱性を ECU メーカーとの緊密な協議に基づいて取り除くことなどが考えられます。こうした措置は無線通信で、フリート内の

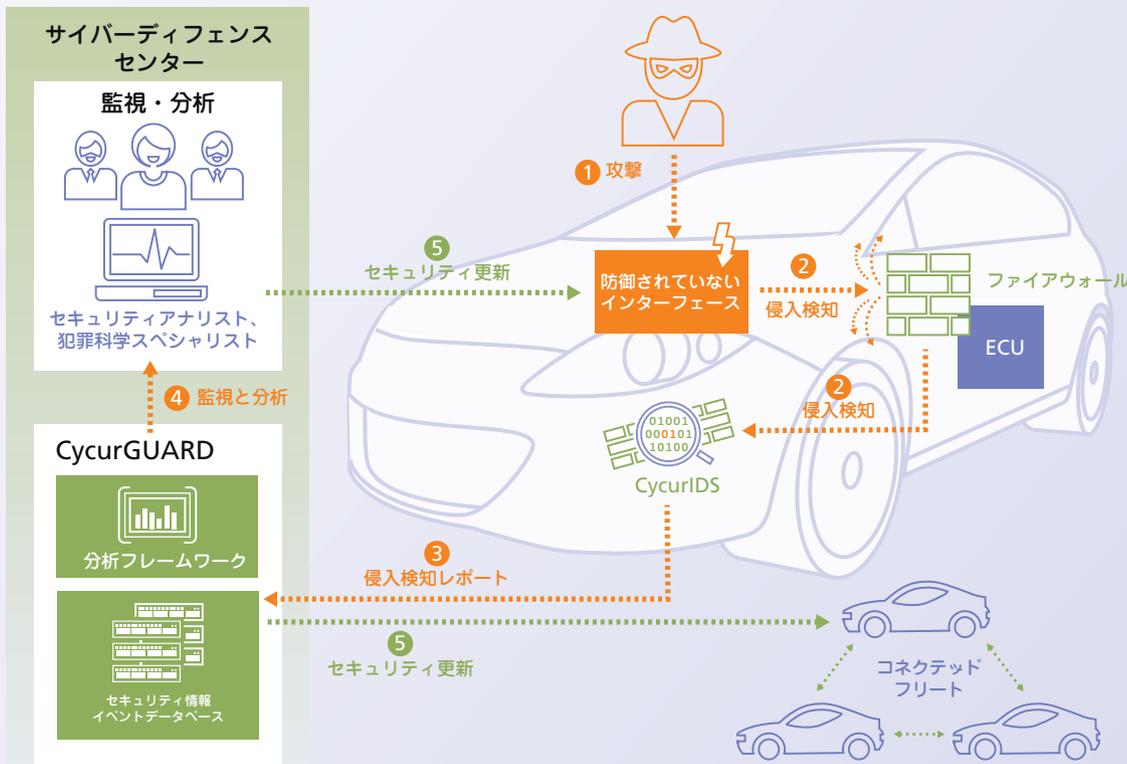
のすべてのコネクテッドビークルに、もちろん暗号化によって保護され伝えられます。さらに、更新情報は気付かないうちに第三者によって変更されることなく、デジタル署名で保護されます。

まとめ

ネットワーク上のすべての車両で検知されたすべての異常に関する情報が、中心となるクラウドベースのイベントデータベースに集められるので、新しい攻撃パターンは即座に識別されます。新たな車両がこのネットワークに接続されるたびに、IDPS はますますインテリジェントになり、脅威に対してより的確な防御策を装備できるようになります。なぜなら、これまで見ることのできなかった攻撃（たとえば、ファイアウォールによってブロックされていた攻撃など）が継続

的な状況評価の対象として送り込まれてくるようになり、以前よりも迅速かつ的確に最新のリスクに的を絞ってセキュリティ対策を適合させることができるようになったからです。この結果、ネットワーク内にはコネクテッドビークル用の免疫システムが構築されます。この免疫システムは新しい攻撃が企てられるたびに強化され、さらに優れた防御を実現していきます。データベースは絶えず拡大を続けている上、防御戦略をフリート内のすべての車両に素早く伝えるので、これまで以上に包括的なオールラウンドの防御を常に確実に実行できるようになります。

予防処置済みフリートへの5ステップ



Embedded Security Testing in Virtual Vehicles

仮想車両で組み込みセキュリティのテストを実施

XiL テスト環境を利用してハッキングを詳細にシミュレート

ソフトウェアで制御される現代の車両システムは、機能的な安全だけでなく、サイバー攻撃に対する防御力も必要です。ハッキングされた ECU がセキュアな状態を保てるかどうかを車両全体についてテストするためのソリューションとして、ETAS と ESCRYPT は仮想化技術に注目しました。ここでは、セキュリティテストに XiL* テクノロジーの長所を生かすことができます。

執筆者

Jürgen Crepin
ETAS GmbH
マーケティング
コミュニケーション
上級エキスパート

Dr. Tobias Kreuzinger
ETAS Inc.
(米国ミシガン州
アナーバー)
テスト・評価上級マネージャ

— ハッカーが車両システムにアクセスしてセンサ信号を傍受し、その信号の代わりに不正なデータを ECU インターフェースに入力する。すると突然、ドライバーは反応することができなくなり、外部からコントロールされた車両の中に閉じ込められてしまう... — このような恐ろしいシナリオをフィクションの世界に留めておくには、信頼できるセキュリティソリューションが必要です。しかし、ハッカー攻撃のテストを行うことなど可能なのでしょうか。つまり、セキュリティ対策が車両システムを確実に防御していることを証明することはできるのでしょうか。機能安全の領域では、通常の運転中も停車中も諸機能が設計どおりに反応することをハードウェアインザループ (HiL) システムで検証することができます。すべての ECU とデータネットワークを含む車両全体のシミュレーションを利用して、ソフトウェアテストや分散されたセンサシステムと車両との相互作用評価を行います。その技術的基礎となるのは、ETAS LABCAR のようなリアルタイム HiL システムや ETAS COSYM コ・シミュレーション、

または ETAS ISOLAR-EVE で生成される仮想 ECU などです。

新しい選択肢： セキュリティインザループ

セキュリティテストの場合、「ツールポジティブ (真陽性) 技法」、つまり予想される挙動のテストは、あまり効果的ではありません。開発の時点では、実際の攻撃シナリオはたいいてい未知のものであり、既知のセキュリティギャップであれば事前に埋めることができるからです。それよりも脆弱性の系統的な探索の方に重点が置かれ、ソフトウェアインザループ (SiL) や HiL のテスト環境はそのような探索にも適しています。そこで課題となるのは、さまざまな領域の能力を融合させる方策です。セキュリティの専門家は XiL のテスト手法をよく理解しておく必要があり、XiL テストエンジニアは従来の IT 環境で用いられる手法について認識しておく必要があります。そうすれば、組み込みシステムに潜在する脆弱性を両方向から認識することができます。ここで特に注目すべきものはセキュリティ関連の車両機能で、その

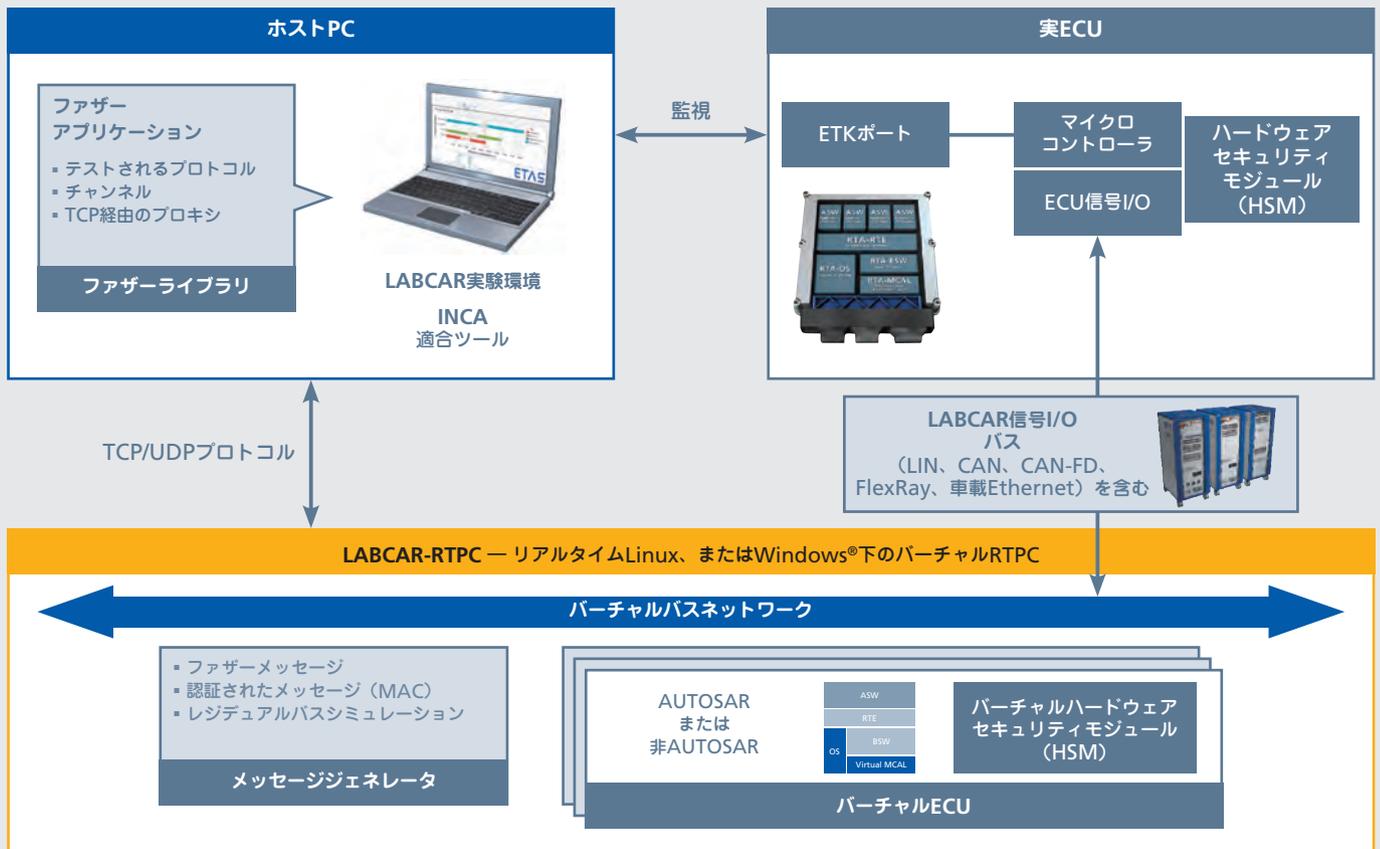
ためのセキュリティテストは最初から一貫性を持って計画し、効率的に実行しなければなりません。ETAS と ESCRYPT は早い段階でこの課題を認識し、安全性や XiL メソッド、自動車セキュリティなどの各分野におけるノウハウを集約し、両者の長所を結集したソリューションを生み出しました (図を参照)。LABCAR ハードウェア、Linux ベースのシミュレーションターゲット LABCAR- RTPC (Real-Time PC)、および仮想 ECU ソリューション ISOLAR-EVE を基礎に構築した仮想テスト環境で、ECU インターフェースに対する攻撃や、ECU の諸機能を不正操作する試みを、車両全体を対象にシミュレートすることができます。

LABCAR を用いたセキュリティテスト

ETAS がテストシステムを提供する一方で、ESCRYPT は以下にあげるように、有意義なテスト手法を選択する際のセキュリティ関連の専門知識を提供します。

- ・ 侵入 (PEN) テスト：このテストでは、外部からの介入で ECU の挙動を不正操作したり、無許可でデータを読み出

* XiL = モデル、ソフトウェア、ハードウェアインザループ (それぞれ MiL, SiL, HiL) の総称



したり、組み込みシステムを破壊したりすることを試みます。半自動化された ETAS と ESCRYPT の PEN テストインザループでは、理想的なテストカバレッジを確保するために「攻撃ライブラリ」を利用します。このライブラリは、ESCRYPT のコンサルティングプロジェクトから得られる経験によって絶えず拡張されています。

- ファジング:** ファザー（テスト実行ソフトウェア）は、ハッカーが ECU ポートをあふれさせようとして送り付けてくるランダム入力や意図的に操作されたコマンドを、自動的に生成します。ハッカーによる侵入や不正操作の試みをシミュレートする際は、一般的に、被験用 ECU のプロトコルやソフトウェアシステム、および暗号セキュリティに関する知識を一体化させて信号生成を行うことにより、テスト効率向上を図ります。
- メッセージ認証 (MAC) テスト:** 認証済みのソースからの入力を用いてシステムにアクセスできるかどうかを調

べます。このテストにおいてテストシステムは、暗号法の暗号鍵やカウンタを生成する機能や、復号時にそれらを解読するためのメカニズムを提供します。

このようなテストでは、個々の ECU や相互接続された複数の ECU の応答から車載 IT システムの脆弱性を系統的に検出することができます。理論上、テストベクタはほぼ無限に存在するので、これを現実的な数に絞り込む必要がありますが、そこで ETAS と ESCRYPT の真価が発揮されます。両者はシミュレーションやテストのためのツールを提供するだけでなく、テスト計画の準備や LABCAR テスト環境の設定に関する適切なサポートも提供しています。ETAS の XiL テクノロジーと ECU アクセス用ツール (ETK など) は、包括的なセキュリティテストを行うために必要不可欠です。テスト担当者は、PEN、ファジング、および MAC テストの実行中に被験 ECU のメモリと内部データの処理に時刻同期でアクセスすることができ、被験 ECU の機能とプロセスを細部にわ

たって完全に追跡することができます。必要な範囲を深く分析できるのは、これらのリアルタイムメカニズムと拡張された監視機能があってこそこのことなのです。

まとめ

ETAS と ESCRYPT は、自動車セキュリティと XiL ベースで行うテストの分野に関する専門知識を長年にわたって築き上げてきました。私たちはこれらの能力を融合させて ECU ネットワークの包括的防御を確実に進めています。XiL システムに有意義なテスト手順を組み合わせることで、セキュリティメカニズムの検証やセキュリティ脆弱性の検出に理想的に適合させることができ、セキュアな未来のコネクテッドピークルの実現に向けた重要なステップをさらに進めることができます。

セキュリティテストシステムの基本構造

次ページでは、**ESCRYPT Testing Laboratory**がコンサルティングとサービスを提供している各種のテストメソッドをご紹介します。

Thoroughly Tested From A to Z

始めから終わりまで徹底的にテスト

執筆者

Dr. Markus Kögel
ESCRYPT GmbH
 エキスパートセキュリティ
 コンサルタント

Dr.-Ing. Marko Wolf
ESCRYPT GmbH
 コンサルティング &
 エンジニアリング
 統括本部長

ESCRYPTは ETAS GmbHの100%子会社です。組み込みシステム向けのセキュリティソリューションを提供しています。

車のライフサイクル全体にわたるセキュリティテスト

効果的な情報セキュリティを実現するためには、車両のライフサイクル全体にわたってセキュリティテストを行う必要があります。なぜなら、従来の安全走行テストでは、主な境界条件が物理法則によって決定され、その後は変わらないことに対し、セキュリティテストでは前提条件と境界条件が攻撃者と防御者の恒久的な争いによって影響されてしまうからです。そのため、セキュリティテストは、車両の量産が開始された後も廃車直前まで定期的に行い、新たに開発されたサイバー攻撃やこれまで検出されていなかったセキュリティホールがないかどうかを調べ、必要に応じて有効な対応を行う必要があります。

この4種類のテストメソッドに分類されます。ESCRYPTはこれらすべての領域について、包括的なコンサルティングとサービスを提供しています。

セキュリティ機能テストでは、使用されているセキュリティメカニズムの仕様が正しく完全に実装されているかどうかを調べます。このステップは一般的な機能テストとよく似ていますが、セキュリティ機能に注目するという点が異なります。そのために、たとえば暗号化アルゴリズムや認証プロトコルなどの実装は、一般的な適合性がテストされ、さらに、たとえばランタイム要件やメモリ容量要件に抵触する可能性を明らかにするため

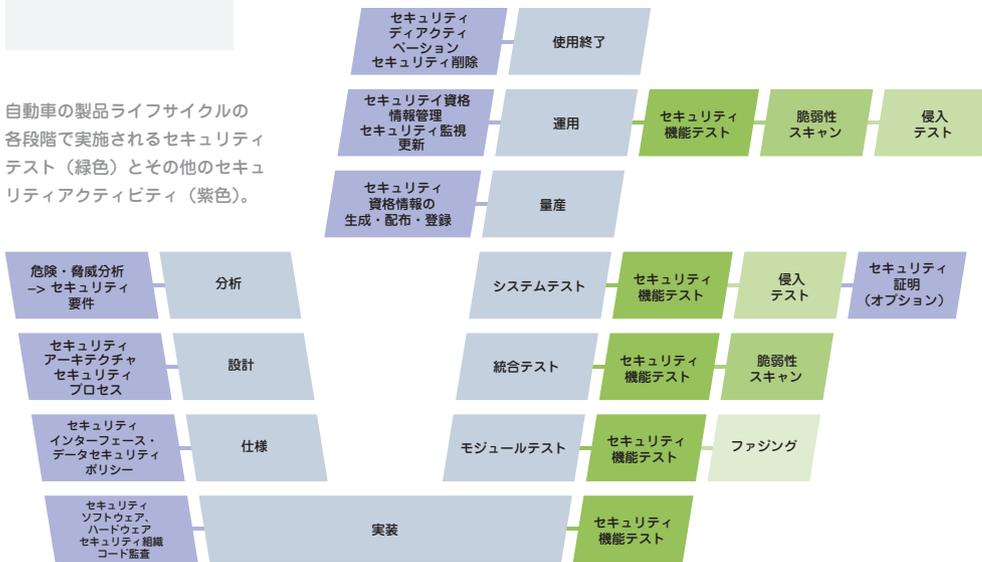
システムの不安定な挙動や誤った挙動を系統的に検知します。

また、脆弱性スキャンでは、システムの共通アクセスポイントや、セキュリティホール、サイバー攻撃に対する脆弱性を調べます。これらのテストでは、テスト時のシステムについて既知のすべての脆弱性情報が常に更新されているデータベースを利用するのが一般的です。

侵入テストは通常、新しい自動車ITシステムのリリース候補（RC）版に対してのみ適用されます。広範にわたるこれらのセキュリティテストは、「人間的なテスト形式として、実際の攻撃者が、利用可能なあらゆる知識、スキル、ツールを利用して見つけたすべての脆弱性に悪用を試みることで、ITシステムを十分にテストすることができる」という基本方針に従って行われます。

ETASとESCRYPTは、コンサルティングやサービスだけでなく、各種のテストシステムも提供しています（12ページからの記事を参照してください）。特にESCRYPTは、10年以上前から自動車セキュリティアプリケーションのセキュリティテストを行っていて、多くのOEMやサプライヤのパートナーになっています。ETASの子会社である同社は最先端のテストラボを擁し、ハードウェア、ソフトウェア、また車載ネットワークの侵入テストの多様なハッキングメソッドに理想的に対処できる設備を整えています。

自動車の製品ライフサイクルの各段階で実施されるセキュリティテスト（緑色）とその他のセキュリティアクティビティ（紫色）。



各開発フェーズに対応する自動車のセキュリティテストメソッド

実際のところ、自動車のセキュリティテストは、図のVモデルの側面に拡張されるセキュリティ機能テスト、自動の脆弱性スキャン、ファジング、侵入テストと

に、実装の性能とリソース消費が監視されます。

ファジングは、セキュリティ機能テストに加えて使用されます。さまざまな予想外の、不正な、また怪しい入力を通して、

A Big Step Forward

大きな一歩

ETAS ASCET-DEVELOPER 7 — 組み込みソフトウェアの安全性向上を手軽に実現

ASCET ならどのような高度な要件があってもワンクリックでソフトウェアコードを生成できる、というのは皆様もすでにご存じのとおりですが、新世代の ASCET-DEVELOPER 7 ではさらにそれ以上のことが実現できます。組み込みシステムのモデルベース開発における安全性、セキュリティ、生産性を新しい水準まで高めることができます。

ETAS の組み込みシステム開発ツール ASCET には歴史があります。第 6 世代の ASCET V6 までですでに 4.5 億件以上の ECU ソフトウェア開発に利用され、その実力を発揮してきました。

そして ETAS はこのツールを大幅に見直し、第 7 世代である ASCET-DEVELOPER 7 として未来へ向けて大きく前進させました。

新世代 ASCET に与えられた目標は容易なものではなく、生産性の向上、プログラミングエラーに対する防御の強化、工業規格への完全順守、ユーザーの開発環境へのシームレスな統合などが求められました。これらの目標を達成するため、オープンな開発プラットフォームである Eclipse の採用や、MISRA-C: 2012/IEC 61508/ISO 26262 などの標準規格への準拠、新しいアイデアによる安全性とセキュリティの強化、ユーザーガイダンスの大幅改良などを行いました。

正確性を「オンザフライ」でチェック
システムの安全関連機能は絶えず複雑化しています。これを制御する組み込みソフトウェアをセキュアに、かつ高コスト効率で行うにはどうすればよいでしょうか。

この問題を解決するのが、専用言語「ESDL」（16 ページからの記事を参照）と「高度な自動化」です。時間と労力を要する手入力作業を省くことで、構文エラーやタイプミス、カンマの位置違い、単位の誤り、といった基本的なエラーを防ぐことができます。またすべてのエントリをオンザフライ機能で自動的にチェックすることで、ゼロ除算や、アンダーフロー／オーバーフロー、配列範囲の超過（インデックスチェックエラー）といった複雑なエラーもすぐに発見でき、速やかに取り除くことができます。ASCET-DEVELOPER 7 はこのような系統的なチェックによりエラーの発生を防ぎます。作成したモデルは開ループと閉

ループのどちらのシミュレーションにも使用でき、プロトタイピングにも利用できます。さらにその後の工程でも、確実性の高い C コードを自動生成することができます。

まとめ：安全性と生産性の向上

ユーザーとの協力によるフィールドテストの結果、ASCET-DEVELOPER 7 を用いれば、その自動化機能と体系的なエラー原因の排除機能によって、従来の ASCET 6 と比べて倍の速さでモデリングを行うことが可能であることがわかりました。

そのうえ、適合性や移植性、さらに最高水準の安全規格への準拠性が向上したことで、ソフトウェアエンジニアは、あらゆる面で保護されたスムーズでストレスのないワークフローに基づいて作業を進めることが可能になりました。

執筆者

Dr. Darren Buttle
ETAS GmbH
ASCET プロダクト
マネージャ

安全性とセキュリティ対策の コーディング



執筆者

Dr. Darren Buttle
ETAS GmbH
ASCET 上級プロダクト
マネージャ

ESDL を用いた、よりセキュアなソフトウェアの実装

組み込みソフトウェアの分野では、プログラミング言語である C 言語が依然として実権を握っています。しかし C コードを確実に安全でセキュアなものにするのは容易なことではありません。高まりつつある車両の自律性に伴い、車載ソフトウェアの完全性への要求度はさらに高まっていきます。ETAS はこのような要求への対応として、組み込みソフトウェア開発言語「ESDL」を開発しました。ESDL は、ISO 26262 や IEC 61508 などの標準規格による制約条件を満たしながらより多くのソフトウェアをより短い時間で開発する手助けとなります。

過去 40 年以上の間、C 言語が組み込みソフトウェア開発用言語の事実上のスタンダードとして扱われています。C 言語はシンプルで軽量であるため、高速で移植性に優れ、幅広いツールに対応しています。

しかし C 言語には負の側面もあります。コード内にエラーが紛れ込みやすい、ということだけでなく、それを見つけて出すのが非常に困難である、ということです。随意的に使用される中括弧や、式における代入、switch 文における意図しないフォールスルーなど、エラーを招く要因が多く存在します。意味的に曖昧であったり複雑であったりする機能については、適切に使用するのが難しく、「危険性のあるプログラミング」(go to 文、ポインタ、整数拡張など)を促すような場合さえあります。これらにより危険な相互作用が引き起こされることも考えられます。

C プログラミングガイドライン (MISRA-C、CERT-C など) に従うことによってこれらの危険の多くを回避することはできますが、それでも C 言語プログラミングにおいてエラーが発生しやすいという傾向は、変わりません。

ガイドラインでは、バッファオーバーフローのような実行時エラーや、アンダーフロー/オーバーフロー、ゼロ除算などといった数値的問題を防ぐことはできません。さらに、制限速度を超えて加速したり、絶対零度以下に温度を下げたり、距離の値に圧力値を加算してしまう、といった機能的なエラーを解決することもできません。

C 言語はそのような情報を表現する能力が充分でないため、上述のような問題を防ぐには、静的なコード分析やテストなどの工程を設けてバグを発見し、取り除かなければならず、それでもまだ十分とは言えません。それよりも最初の段階からバグの発生を阻止する方がはるかに効果的です。

より優れた開発言語の提供

ETAS は、安全でセキュアなソフトウェアを効率的に設計できる ESDL (Embedded Software Development Language) という新しい言語により、前述のすべての問題に対処しています。ESDL は C 言語にありがちなトラブルを解消できるだけでなく、ソフトウェアの再利用が可能になるため、保守性が向上し、製品ライン内の複数のバリエーションへの対応も可能です。つまり、これまで C 言語の欠点への対処に費やしていた時間を、本来の機能的問題の解決に利用することができるのです。

コードジェネレータによる C コード生成

開発工程における ESDL の効率的な利用は、ETAS ASCET-DEVELOPER 7 (15 ページの記事を参照) と Eclipse ベースの統合開発環境 (IDE)、および C コードジェネレータによって実現します。

IDE には、言語テンプレート、コンテンツアシスト、問題のクイックフィックスなどの先進的な編集機能が含まれているので、初心者でも ESDL を容易に習得することができます。ASCET-DEVELOPER 7 は、ESDL のプログラミング違反がないかどうかをチェックし、品質メトリクスの計算、ベストプラクティス推奨事項の提案なども継続的に行います。編集集中に「オンザフライ」でフィードバックが提供されるので、コーディングミスがあってもユーザーが即時に対処することができます。

C コードジェネレータは、ESDL を MISRA 準拠の C コードに変換します。ASCET-DEVELOPER 7 は、実行時の安全性を確保する上で不可欠となる箇所にコーディングエラーをチェックするために防衛的コードを自動的に挿入するので、手作業でのチェックコードの作成や保守は必要ありません。こうして生成された C コードは、既存の C 言語開発工程に容易に統合することができます。

コードの潜在的エラーを防ぐ

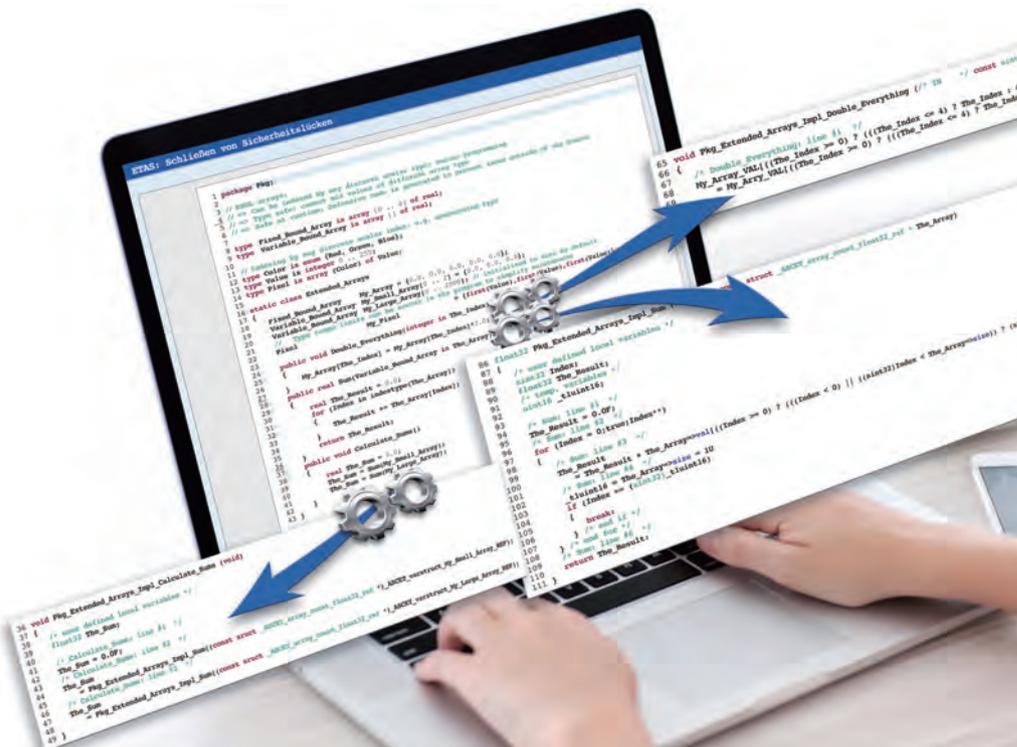
ESDL には、C プログラミングガイドラインに含まれる機能が多く組み込まれています。さらに ESDL には、ISO 26262 や IEC 61508 といった標準規格で定められている言語選択の要件を容易に満たすことができる機能が含まれています。ESDL に組み込まれたこれらのコンセプトにより、開発ツールである ASCET-DEVELOPER 7 での編集時に、従来の C 言語開発よりも多くのエラーケースをチェックすることが可能になりました。

ESDL の構文は C 言語とよく似ているので、すぐに快適に使用することができます。ただし、一般的にガイドラインによって使用を制限または禁止している危険な C 言語の構文は排除されています。ESDL には、随意的な中括弧や、ステートメントとしての式の使用、ループ変数への代入、switch 文のフォールスルー、暗黙的な整数拡張、グローバル変数、ポインタ、go to 文、共用体、といった危険要素は存在しません。そのため、本質的に C 言語よりも安全に使用することができます。

ESDL で記述された計算は、アンダーフロー、オーバーフロー、ゼロ除算、符号付き算術演算のオーバーフロー、といった数値に関する一般的な問題とは完全に無縁です。

ESDL では、境界を越えた配列アクセスが発生することはありません。多くのセキュリティレポートに見られるバッファオーバーフローも発生し得ません。

ESDL には、C 言語の typedef のように、名前を型に割り当てる拡張可能な型システムがあり、許容値の範囲と、必要に応じて分解能に関する情報を追加定義することができます。たとえば「speed」を、値の範囲が 0.0 ~ 260.0 km/h で分解能が 0.01 km/h の実数型として定義することができ、型の単位として meters (メートル)、degrees (度)、time (時間) などを使用することができます。



セキュリティギャップも、プログラミングしながら素早く埋めることができます。

の工程で発見されると、それを取り除くのは容易ではなく、非効率的です。C言語で開発するエンジニアは、往々にしてこのようなC言語の不備への対処に膨大な時間を費やしている、と言えるでしょう。

ETASは、ESDLとASCET-DEVELOPER 7の組み合わせにより、安全でセキュアなCコードをより効果的かつ効率的に作成できるようにしました。ESDLはあらゆる種類の潜在的エラー原因を排除し、複数のプロジェクトでのソフトウェアの再利用を容易にします。ESDLにより、組み込みソフトウェア開発の効率性、安全性、セキュリティ対策は、新しい水準に到達しました。

「時間を距離に加算してしまう」といった誤りを防ぐため、単位の整合性が自動的にチェックされます。ASCET-DEVELOPER 7のコードジェネレータは、ESDLの型情報に基づき、値を保存するのに最も適したCデータ型を選択し、実行時に常に値が妥当であることを保証するための防衛的チェックコードを生成します。

プログラム内の1カ所で変更を行えば、Cコードを再生成するだけでシステム全体にその変更を適用することができます。これによってレビューや検査も容易になります。またESDLプログラムは、実際の処理内容を捉えにくくする手書きの範囲チェックによって可読性が落ちる心配もありません。

データアクセス制御と再利用化

オブジェクトベースの言語であるESDLは、クラスを用いてデータアクセスの管理と制御を行います。オブジェクトは安全かつセキュアに使用することができ、メモリ境界も既知のものとして管理されます。ESDLにはC++やJavaのような

動的ストレージアロケーション機能がないので、メモリリークも発生しません。

ESDLのクラスは、複製して改変することなく、製品ラインの別のバリエーションに利用することができます。以下のようなバリエーションが可能です。

- コード
- データ初期化
- メモリアロケーション
- Cデータ型（浮動小数点から固定小数点へ、またはその逆の変更など）

リアルタイム環境におけるデータの整合性は、ESDLでは「メッセージ」と呼ばれるスレッドセーフな通信メカニズムで実現しています。メッセージには読み手と書き手が明確に定義され、定義されていないデータアクセスは行えません。

結論

車両のコネクテッド化に対応する複雑な開発環境では、プログラミング言語であるC言語の特徴である「柔軟性」がデメリットとなる場合があります。コードに入り込みそのまま放置されたエラーが後



Virtual ECUs in Production Vehicles?

量産車に仮想 ECU を搭載？

執筆者

Michael Hauser 氏
Bosch Automotive
Electronics

(シュトゥットガルト)
 ソフトウェア開発チーム
 リーダー

Dr. James Dickie
ETAS Ltd

(英国、ヨーク)
 RTA ソリューションズプロ
 ダクトマネージャ

Dr. Nigel Tracey
ETAS Ltd

(英国、ヨーク)
 統括マネージャ

ETAS Lightweight Hypervisor による柔軟性、高効率性、セキュリティ対策の実現

「アジャイルソフトウェア開発」は、自動車産業界において採用が増えている開発手法です。この手法は「安全性やセキュリティ対策を気にせずに、ユーザーがソフトウェア制御式の車両ファンクションのアップグレードや更新を行える」という発想に基づきますが、これはソフトウェアファンクション同士が厳重に分離されていることが前提となります。しかしハードウェアの傾向はこれに反し、中心的な複数の ECU においてますます多くのファンクションが実行されるようになってきています。このギャップを解決するため、Bosch Automotive Electronics は ETAS の新しい軽量ハイパーバイザを採用しました。

免許取得から 3 年、無事故で安全運転を続けた Leon に、ついにその日がやってきました。両親は彼の車のメーカーのウェブサイトにログオンし、免許取得時にオンに設定してあったソフトウェア制御式パワーリミッタをオフにします。同時に、Leon が欲しがっていた新しいマルチメディアパッケージのインストールも行います。この費用は彼も半分負担します。

車両の納品後にこのようなファンクションアップグレードを行い、無線通信経由 (OTA: over-the-air) で継続的な更

新が行えるようにするには、その影響が他のソフトウェアに及ばないことが前提条件となりますが、これまで以上にコネクテッド化された多くのファンクションが複数の中心的 ECU に集中する傾向にある今日、それを保証する手段はあるのでしょうか。さらに、アップグレードや更新を行った後にシステム全体の機能安全を走行前に検証することはできるのでしょうか。この 2 つの質問は、ソフトウェアファンクション間の確実な分離が非常に重要であることを示しています。

実質的なパーティショニングが必要

このような「分離」が支持される理由は、機能安全以外にもあります。厳密に分割されていれば、たとえば複数のメーカーのソフトウェアが同一 ECU 上で実行される場合に、開発時のワークフローを単純化することができます。またファンクションの分離によって ECU への攻撃が難しくなるため、サイバー犯罪が増加している現代では重要なファクタであると言えます。あるファンクションにハッカーがアクセスすると、その行く手にハイパーバイザが高いハードルを配置し、

最大の損害を与えようとするサイバー犯罪者の意欲を強力に抑止します。「分離」はさまざまな手法で実現することができます。まずはソフトウェアファンクションをそれぞれ専用の制御ハードウェアに厳密に割り振ることが考えられますが、それではハードウェアのコストとシステムの複雑性が桁違いに増大してしまいます。より現実的な手法として、「パーティショニング」と「分離」のコンセプトが定義されているAUTOSARベースのアーキテクチャがあります。これにより、他のファンクションに影響を与えずに個々のファンクションをアップグレードすることが可能になります。この手法では、1つのファンクションが修正されるたびに同じECU上のソフトウェア全体を包括的に再検証する必要がなくなります。ただしこのAUTOSARのコンセプトを実装するにはアドオンが必要です。

ハイパーバイザが提供する解決策

ここでハイパーバイザによる効果的な解決策をご紹介します。ハイパーバイザは1つのECUを複数の仮想マシン（VM: Virtual Machine）に分割します。実際には複数のファンクションが同じECU上で実行されるのですが、ソフトウェアは各ファンクションに専用のハードウェアが割り振られていることを認識しています。ファンクション同士は非常に厳密に分離されているので、個別に修正でき、修正後にシステム全体を再検証する必要はありません。またソフトウェアサプライヤは、ECUの開発時において他のどのサプライヤとも無関係に作業することができます。ソフトウェアエラーや悪質な侵入者が出現しても、1つの仮想マシン上に局所的に封じ込めるため、拡散することはありません。また、最低レベル（QM）から最高レベル（ASIL D）までのさまざまなASIL（Automotive Safety Integrity Level: 安全性要求レベル）のソフトウェアを1つのECU上で動作させることが可能になります。ただし、ハイパーバイザソリューションのすべての長所をうまく生かせるかどうかは、その実装方法に依存します。このソリューションを実際の車載環境に適合

させないと、不具合が生じる可能性があります。たとえば、アクセス許可を制御するには、通常はハイパーバイザ専用のメモリ管理とハイパーバイザ特権モードが必要です。従来のバージョンでは3段階の特権モード（ハイパーバイザ自身、基本ソフトウェア、適合ファンクション）があります。しかし一般的な車載マイクロコントローラはこれらのメモリ管理や3段階の特権モードに対応していないため、今日までハイパーバイザテクノロジーが車載システムで幅広く使用されることはありませんでした。

ある大規模OEM向けのプロジェクトにおいてBosch Automotive Electronics - Body Electronics (AE-BE) は、ETASの軽量ハイパーバイザ（ETAS RTA-LWHVR）と共にようやくこの問題を解消することができました。最適化により、自動車用ハイパーバイザのメモリ使用量が5キロバイト（kB）に抑えられただけでなく、アクセスタイムも4～5倍改善されました。そしてこの新しいソリューションは、仮想マシン間の影響をなくしました。このプロジェクトでは、中心的なボディECUが11個の仮想マシンに分割され、各仮想マシンがそれぞれ異なるサプライヤのソフトウェア用に確保されました。ASILの等級範囲はQM～Bです。

AUTOSARを超える 軽量ハイパーバイザ

システムには多種多様なソフトウェアファンクションが数多く存在していましたが、軽量ハイパーバイザがそれらをカプセル化し、すべて問題なく機能しています。仮想マシンが共有メモリにアクセスしても、そのアクセスとランタイムがコア上で明確に制御されるのです。

このソリューションでは、コンピュータコアを1つのマスタコアと複数のアプリケーションコアに分割することで高性能を実現しています。マスタコアに与えられるジョブとしては、ハードウェア管理や、中央の基本ソフトウェアと各種のソフトウェアアプリケーションの実行が

あり、各アプリケーションコアには厳密に分離された複数の仮想マシンが展開されます（図1参照）。各仮想マシンは、パーティション化されたAUTOSARランタイム環境（RTE）またはAUTOSAR非準拠のソフトウェアで構成され、これらすべてが1つのECU上で実行されます。このアプローチにおいてはBosch AE-BEが開発したコア間通信（ICC）が重要な役割を果たします。どのような状況においても実行時間が保証されるだけでなく、各ファンクションは、他のファンクションの実行を抑制することなくタイムバジェットを追加要求することができます（図2を参照）、リアルタイム要件は常に保証されます。

高度なランタイム要件により仮想マシンの能力を超える負荷が発生する恐れが生じると、仮想マシンはハイパーバイザに対して、予備のランタイムウィンドウに一時的にアクセスしてよいかを尋ねる場合があります。するとハイパーバイザは、予備のランタイムウィンドウが利用可能になるのを待つためのキューにその仮想マシンを追加します。そしてランタイムウィンドウが解放されると、ハイパーバイザはキューに最初に入れた仮想マシンにそのウィンドウの使用を許可し、システムの高負荷による影響を最小限に抑えます。ただし、不正な仮想マシンがシステムの支配権を得ようとするのを防ぐため、各仮想マシンは1つの予備ウィンドウの使用しか要求できません。

今日から使える未来型ソリューション

標準的なハイパーバイザに比べて、メモリーオーバーヘッドはわずか5kBに低減し、電力消費もコアの使用可能容量の5パーセントに抑えられました。このような改良により、RTA-LWHVRは車載組み込みシステムの境界条件に難なく適合することができます。柔軟性に富んでいるため、広範なアプリケーションに対応でき、数多くのマイクロコントローラに実装することができます。また高性能かつ高信頼性のパーティショニング技術でECUを分割するので、今後は、さまざまなメーカーやさまざまな安全等級のソフトウェアを同一のECU上で稼働させ

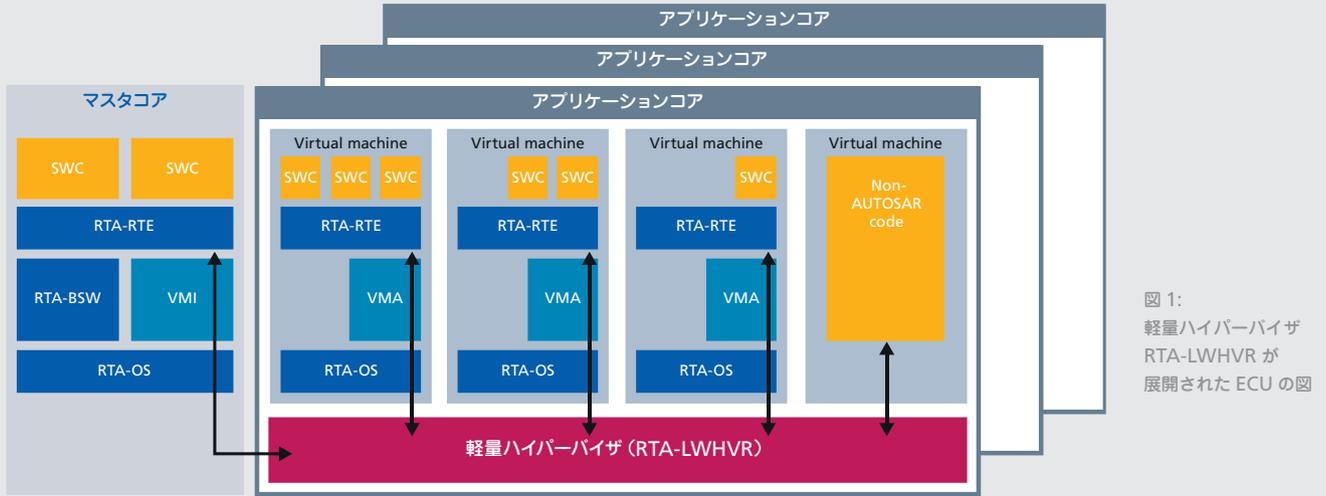
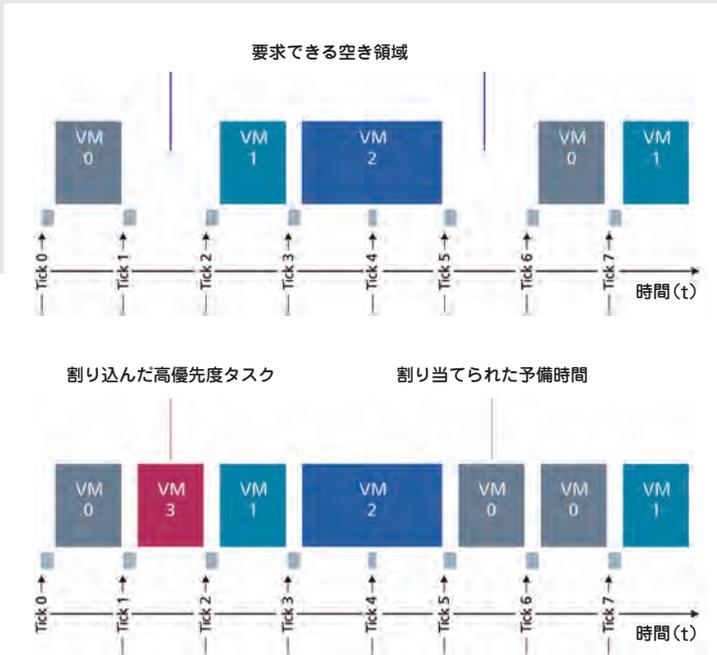


図 1:
軽量ハイパーバイザ
RTA-LWHVR が
展開された ECU の図



RTA-BSW AUTOSAR基本ソフトウェア
 RTA-OS オペレーティングシステム
 RTA-RTE ランタイム環境
 SWC セキュアアプリケーションのソフトウェアコンポーネント
 VMA 仮想マシンアダプタ
 VMI 仮想マシンインターフェース
 → コア間通信 (ICC)

VM 仮想マシン

図 2:
アプリケーションコア内の時間管理

ることができるようになります。

インテリジェントなコア間通信と厳密なカプセル化により、ソフトウェアで制御する複数のファンクションを互いに影響されずに開発することができます。既存車両のファンクションも含めた修正も容易に行え、時間のかかるシステム全体の再検証を行う必要がなくなります。このように軽量ハイパーバイザは、自動車産業界においてソフトウェアとファンクションのアジャイル開発を行うためのセ

キュな基礎を構築するので、定期的なセキュリティ更新を行う動的セキュリティシステムも容易に実現できます。そして、Leon と彼の両親が利用したような車両の設定変更やアップグレードを実現すること阻むあらゆる障害を取り除くことも可能になるのです。

Continuous Delivery of ECU Software

ECU ソフトウェアの 継続的納入

電動化を促進するアジャイルソフトウェア開発

低公害車に対する需要は常に増大し続けており、OEM はこの大規模市場に対応して新しいハイブリッドモデルや電動モデルを開発しています。Robert Bosch Mobility Solutions のパワーエレクトロニクス事業部（GS-PE）では、そこで頻繁に求められる新しい要件に応えるため、高い俊敏性を持ってパワートレインへの効率的な電力供給システムを開発しています。そして、開発された新しいファンクションと最適化された ECU ロジックについて、継続的な改良、テスト、リリースを行っています。

執筆者

**M.Sc. Jochen
Horinek 氏
Robert Bosch
GmbH**

GS-PE 事業部
ソフトウェアテスト
エキスパート

**Dipl.-Ing. Jörg
Spranger 氏
Robert Bosch
GmbH**

GS-PE 事業部
ソフトウェア開発
エキスパート

この開発を実現するため、パワーエレクトロニクス事業部ではインバータ ECU 用ファンクションの開発、統合、テストの高度な自動化と並列化を行いました。この基礎となっているのは、アプリケーションライフサイクルマネジメント（ALM）ツール環境です。この環境は、顧客の要求、報告されたエラー、テストケース、テストレポートなどの情報を開発者とテスト担当者に提供するもので、すべての「作業指示」が ALM 内で追跡されます。開発者は作業指示の情報に基づき、ETAS ASCET を使用して AUTOSAR 準拠の ECU ファンクション用ソフトウェアコンポーネントの作成や修正を行います。

ソフトウェアのテストとリリースを継続的に実行

新しく作成されたソフトウェアコンポーネントや修正された既存のソフトウェアコンポーネントは、システムにチェックインされ、即時に ECU ソフトウェアに統合されます。続いて静的解析が行われ、各コンポーネントについてコーディングミスの有無とコーディングガイドラインへの適合性が自動的にテストされます。テストに合格すると、ETAS INCA を用いて新しいソフトウェアバージョンを

ECU に適合させ、さらに ETAS DESK-LABCAR 上でリアルタイムソフトウェアシミュレーションによる ECU の閉ループテストを行います。すべてのテストに合格したソフトウェアバージョンは、リリースされ、高電圧のテストベンチでさらに検証されることになります。

メリット

ファンクション開発の工程は、新規ファンクションのテストであっても、統合からレポート生成までを完全に自動化することができます。具体的には、作成または修正したソフトウェアコンポーネントを夕方にシステムにアップロードすれば、その夜の間に自動テストを実行することができます。翌朝、エンジニアはテスト結果を確認し、コンポーネントを修正する必要があるかどうかを判断します。テストに合格したコンポーネントは、テストラン完了後に新しいソフトウェアバージョンに統合されます。このソフトウェアバージョンは ECU 上で直ちに実行できるため、実験室でのさらなるテストやその後の車載テストにも利用できます。テストにおいては、高性能でコンパクト、しかもコスト効率の高い DESK-LABCAR システムが有用で、多くのハードウェアインザループテストを並列化

することができます。

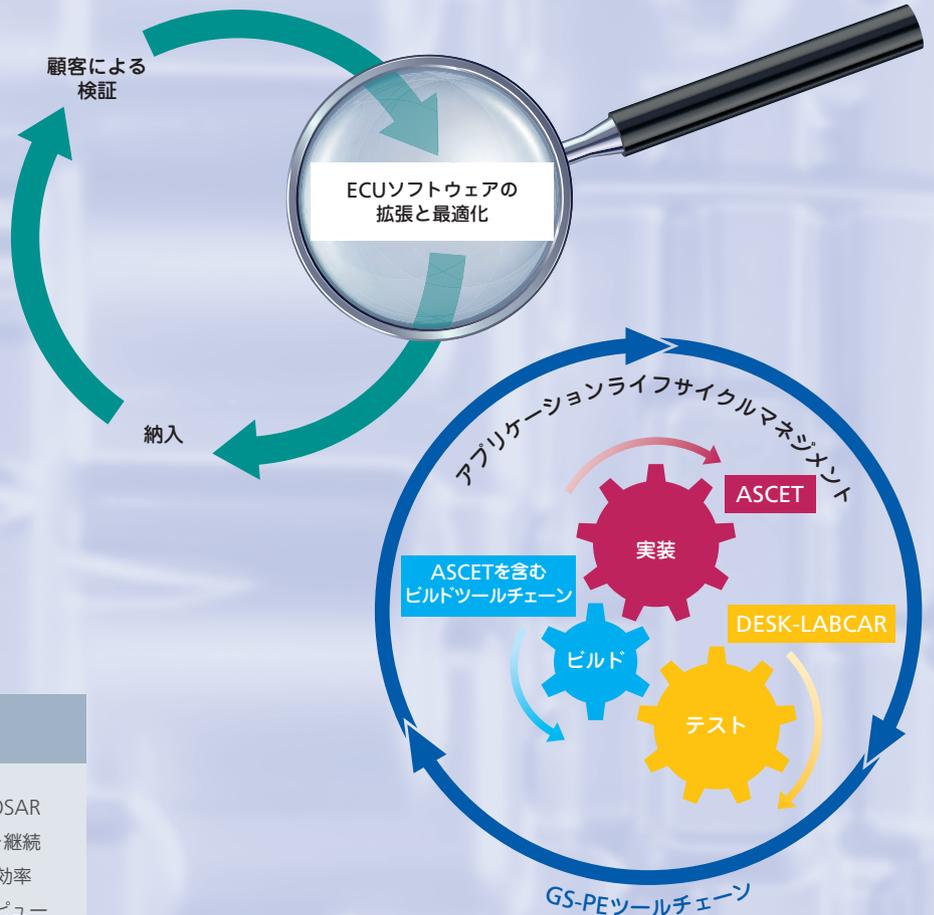
顧客の利益

インバータ ECU 用ソフトウェアの継続納入は、電動パワートレイン用システムのアジャイル型共同開発を大いに後押しするものです。頻繁にリリースされるソフトウェアバージョンをすぐにターゲットシステムへ提供できるので、ソリューションの開発と最適化を顧客と綿密に相談しながら進めていくことができます。

GS-PE 事業部の
ツールチェーン（右図中央）が、
インバータ ECU 用ソフトウェアの
継続的な開発と納入（右図左上）を
実現しています。

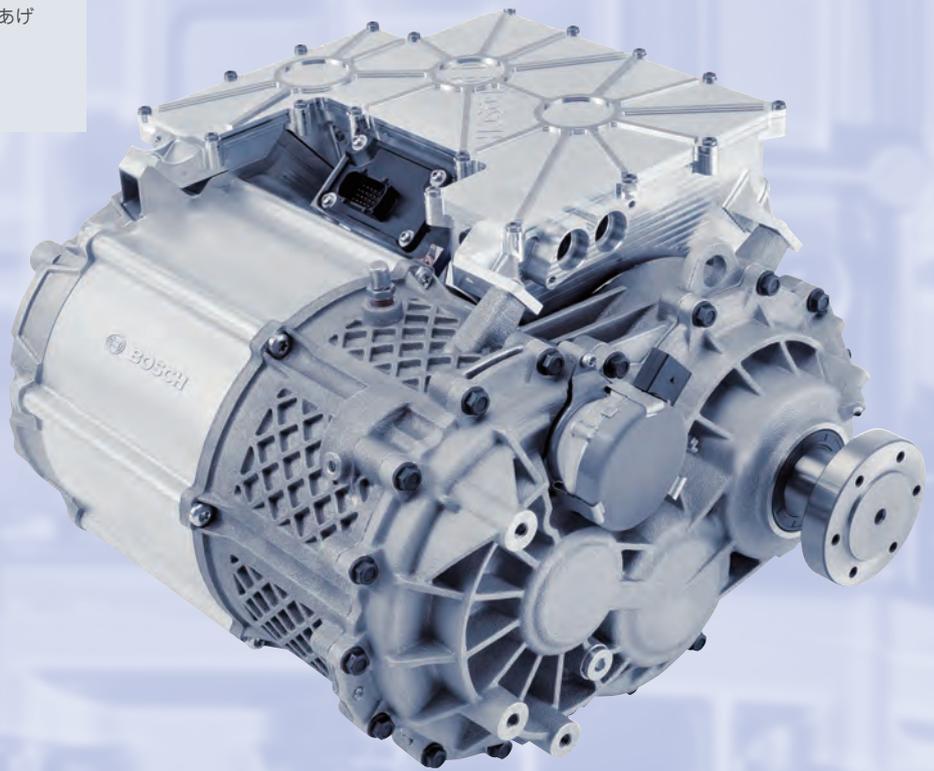
このツールチェーンでは、
ASCET を使用してファンクションを
新規に実装または修正し、
それをソフトウェアに自動的に統合して
テストすることができます。

この工程では
アプリケーションライフサイクル
マネジメントシステムが活用され、
関連するすべてのデータの
保管と処理に利用されています。



今後の展望

ETAS ISOLAR-EVE を使用して生成できる仮想的な AUTOSAR ECU を利用することにより、今後も ECU ソフトウェアを継続的に納入し、さらに効率の向上を図ることができます。「効率向上」の一例として、ECU ハードウェアを使用せずにコンピュータ上の仮想環境で ECU ソフトウェアをテストすることがあげられます。



Bosch の新しいソリューション「eAxle」:

GS-PE 事業部門は、
モーター、パワーエレクトロニクス、
トランスミッションを一体化しました。

このパワートレインにより
50 ~ 300 キロワットの電力を
供給することができます。

GS-PE は、ASCET と LABCAR を利用して
この軽量でコンパクトなアクスルドライブを
制御するソフトウェアの開発と
テストを行っています。

New Paths Through the Function Labyrinth

ファンクションの迷宮を抜ける 新たな道筋

ファンクション開発という迷宮から早く抜け出す方法を模索するには、さまざまなツールが役立ちます。その中で新たな選択肢であるETASのSCODE-ANALYZERとSCODE-CONGRAは、まったく新しい手法のソフトウェアツールです。これらの独特なツールを利用して迷宮を簡単に切り抜ける方法を詳しくご紹介しましょう。

Methodology

The tools are based on the approach of functional morphology – that is, studying the structure of functions and their relationships with each other; and automated cognition – the reorganization of information in a system that controls behavior.

Enthusiasm

The team that brought the prototypical tools from research to the production stage in ten years of development work had a lofty goal. Their ambition was to rewrite the book of embedded software development – and we think they have achieved it.

What benefits do the new tools bring?

They free up developers from simple routine tasks, such as analyzing dependencies, solving equations, and generating code for the next work steps. Furthermore, they support creativity to find the best solution.

Fields of application

System, function, and software developers can describe, visualize, analyze, and optimize their complex systems from the very start of the development process.

Reaching your goal faster

Initial projects have shown that the work involved in function development can be reduced by more than **30%** in some cases with SCODE-ANALYZER and SCODE-CONGRA.

Simulink® connection

SCODE-ANALYZER and SCODE-CONGRA can be integrated easily into MATLAB®/Simulink® environments. Both tools generate code that can be further processed in MATLAB®/Simulink®.

Demonstrably safe

Automatic verification of the complete description of the decision paths and mathematical relationships supports the requirements for proving functional safety as per ISO 26262. The completeness of the analysis is mathematically demonstrated – that is unique.

執筆者

Jürgen Crepin**ETAS GmbH**

マーケティング

コミュニケーション

上級エキスパート

Goethe, Zwicky, and Michael Jackson?

Taking a long view, the story of SCODE-ANALYZER and SCODE-CONGRA begins in the 18th century. In his studies of morphology, Johann Wolfgang von Goethe described the relationships of the various forms of life on our planet. This basic idea inspired Bosch researchers from the fields of mathematics, computer science, engineering, and philosophy. SCODE-ANALYZER and SCODE-CONGRA were influenced by ideas from the astronomer Fritz Zwicky, the scientists Stephen M. McMenamin and John F. Palmer, and the British computer scientists Michael Jackson and George J. Friedman – augmented by the graph theory of Markus Behle, the product manager responsible for the software tools.

Eclipse and ready to go
Using Eclipse interfaces, the new tools can be easily integrated into existing tool chains.

Secure connection
The tools' interdisciplinary approach brings together the separate paradigms of classic IT development and the development of closed-loop control functions.

Always at your service
ETAS also offers consulting services to help you familiarize yourself with the new methodology and to use the new tools efficiently.

Curious? Find out more at etas.com/scode, etas.com/congra, or listen to the ETAS Expert Talk playlist on our YouTube channel.

SCODE-ANALYZER (System CO DEsign)

このツールを使用すると、あらゆる種類のシステムの複雑な関係性を、明快に構造化して記述し分析することができます。この手法では、システムをいくつかの「モード」と呼ばれる動作領域に分割します。特に、判断箇所やバリエーションの多いソフトウェアにはこの手法が有利で、複雑性を大幅に低減することができます。

SCODE-CONGRA (CONstraint GRaphs)

SCODE-ANALYZER アドオンの SCODE-CONGRA を使用することで、ファンクション開発担当者は、正確な数学に基づき、理解しやすい用語で明快にシステムの記述と図式化を行うことができます。システムのルール違反、矛盾、代数ループなどの重要な特性が正確に表示され、エラーを訂正するためのオプションや機能が提供されます。変更内容がシステムに与える影響も、非常に理解しやすい形で表示されます。コンポーネントを個別に修正しながら実験できるので、短期間でさまざまなバリエーションを試して評価することができます。

適合エンジニアに対しては、事前適合済みの的確なパラメータが提供されます。重要な動作ポイントにおけるシステムの反応が示されるので、システムの重要箇所に絞って適合作業を行うことができ、事前適合済みのパラメータを実際の動作条件下で最適化することができます。

Simulation and Virtualization of Vehicle Systems

車両システムの シミュレーションと仮想化

執筆者

Dr. Ulrich Lauff
ETAS GmbH
マーケティング
コミュニケーション
上級エキスパート

Dr. Christoph Stoermer
ETAS GmbH
先行開発部長

Deepa Vijayaraghavan
ETAS GmbH
上級プロダクトマネージャ
テスト・評価
ソリューション責任者

分散化 ECU ファンクションの開発とテストを ETAS COSYM で

複数の車両電子制御システムを一体化した自動運転の諸機能について、競争力ある価格と品質を維持しながら速やかに本格生産へつなげるにはどうすればよいでしょうか。また、電気エンジンや燃焼エンジン、バッテリー、触媒コンバータ、自動変速装置などで構成される複雑な駆動システムに最適なデザインとは、いったいどのようなものなのでしょうか。

MiL/SiL や HiL の環境で、新しい機能をシームレスに開発し、柔軟性のあるテストを行うには、仮想 ECU を生成できる強力な環境や、モジュラー構造のシステムモデルの統合と設定を行える高度なツールのほか、シミュレーションを行うための拡張性に富んだプラットフォームが必要です。

ETAS COSYM

COSYM を使用すれば、ネットワークに接続した組み込みシステムのテストと検証を仮想環境で効率的に行え、さらに新しいソフトウェアテクノロジーを基礎とするオープンなシミュレーションプラットフォームを利用することができます（図を参照）。中核機能としては、ECU ネットワークの状態に注目しながら包括的な MiL/SiL/HiL (XiL) システムテストが実行でき、さらに、システムとソフトウェアの開発工程における最新の「継続的インテグレーション」(CI: Continuous Integration) のためのプラットフォームも提供します。

COSYM には、以下の処理を行うためのツールが付属しています。

- プラントモデルや ECU ファンクション、「レストバス」モデル（当該ノード以外の部分をシミュレートするモデル）、信号接続情報などをインポートし、システムモデルを作成します。仮想ネットワークを作成して仮想 ECU

や実際の ECU に接続するオプションもあります。生成されたシステムモデルでは、モデル信号の結合だけでなくネットワーク通信も考慮に入れることができます。ETAS ISOLAR-EVE などを用いて仮想 ECU をマイクロコントローラの抽象化レベルで統合すれば、アプリケーションソフトウェアレベルで統合した場合に比べてより正確なシミュレーションが行えます。

- 実行時のプラットフォームとタイムフレーム（リアルタイムまたはシミュレーション用タイムスケール）に基づき、シミュレーションを MiL/SiL/HiL 環境用に設定します。
- ETAS の実験環境を利用して実験を実行します。
- XiL API または標準の REST インターフェースによる自動化を行います。これにより、継続的インテグレーション環境で最先端のソフトウェア実装を行うことができます。COSYM ではサーバー上にプロジェクトを作成することができ、将来的にはそこで実験を行うことも可能になる見込みです。

最新のソフトウェアテクノロジーを応用した COSYM では、「サービス」と「ユーザーガイドランス」とが一貫して分離されています。定評のある REST サービスインターフェースは、ユーザー独自のユーザーガイドランスや自動化処理に容易に統合することができます。また COSYM

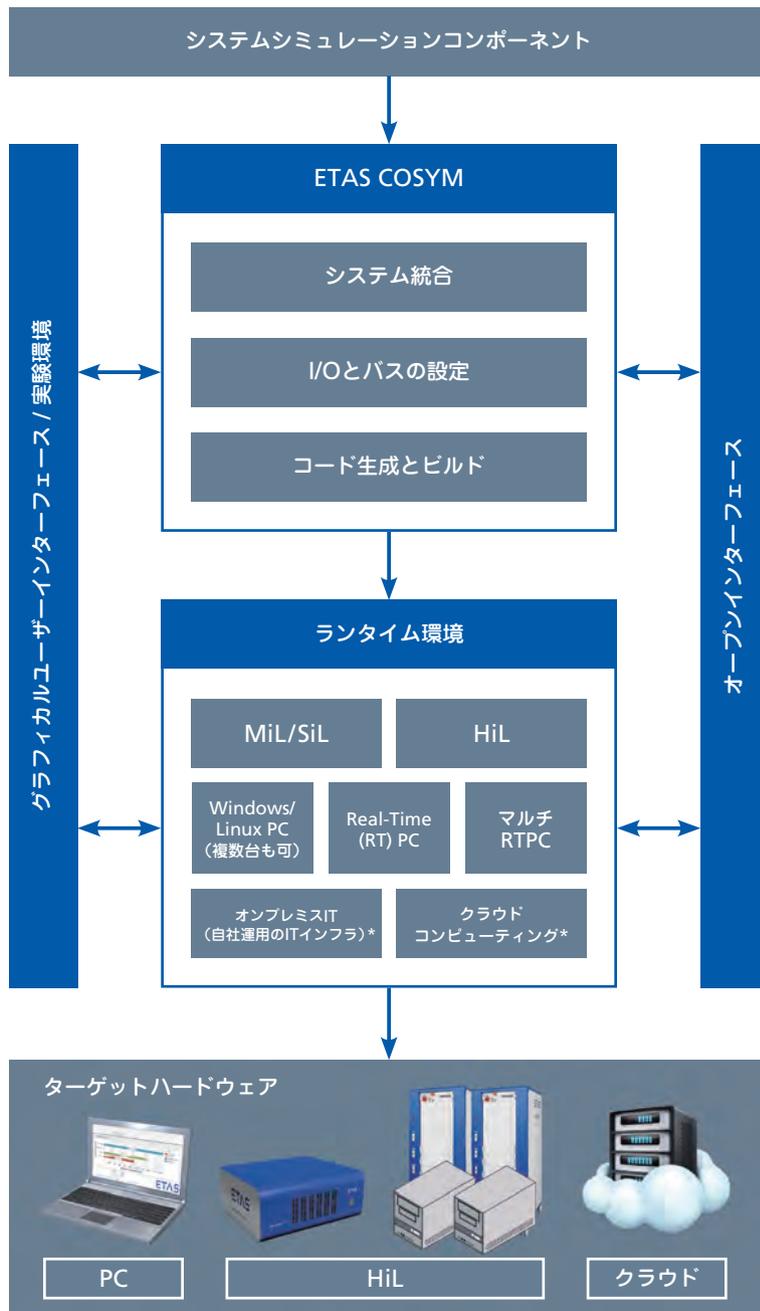
にはウェブベースのユーザーインターフェースが標準装備されています。サービス志向アーキテクチャを採用したプラットフォームは、Eclipse などのような統合開発環境 (IDE) に組み込むことが可能です。

市場への投入

COSYM のリリースは、パイロットプロジェクトの一環として 3 段階で行っていきます。まず第 1 段階として、2017 年末には ETAS LABCAR HiL システム用のものを発売する予定で、これにより HiL テストを仮想環境 (PC 上など) にすべて移し替えることが可能になります。たとえば LABCAR-MODEL ファミリのプラントシミュレーションを移し替え、さらに実際の ECU を仮想 ECU やファンクションモデルに置き換えれば、システム全体を仮想化することができます。

第 2 段階として、2018 年中頃までには標準的なすべての車載バスの仮想ネットワークを統合可能にする予定です。さらに、リアルタイムシミュレーションに代わる「仮想タイムスケール」を COSYM と LABCAR-MODEL に導入する予定で、HiL でのリアルタイムテストよりも高速なテストが可能になります。

2018 年中頃以降は、最後の第 3 段階として、複雑なシステムの適合を仮想環境で行うための基礎を築いていく予定です。



ETAS COSYM — システムの概要

す。ここでは2つの大きな目標があります。第1に実路走行排気（RDE）に関するテストが可能になること、そして第2に、路上試験時の測定データなどを利用して、ADASや運転自動化アプリケーションの調整とテストが仮想環境で行えるようになることです。

今後の展望

中期的には、COSYMプラットフォームを拡張し、高性能のサーバーインフラストラクチャ（自社運用のサーバーなど）にも実装できるようにする予定です。多量のデータを必要とする自動運転システム開発をよりの確にサポートする目的でビッグデータソリューションの統合にも重点を置いているので、膨大なデータセットの中からシミュレーションとの比較や融合に適した測定データを迅速に選び出すことが可能になります。

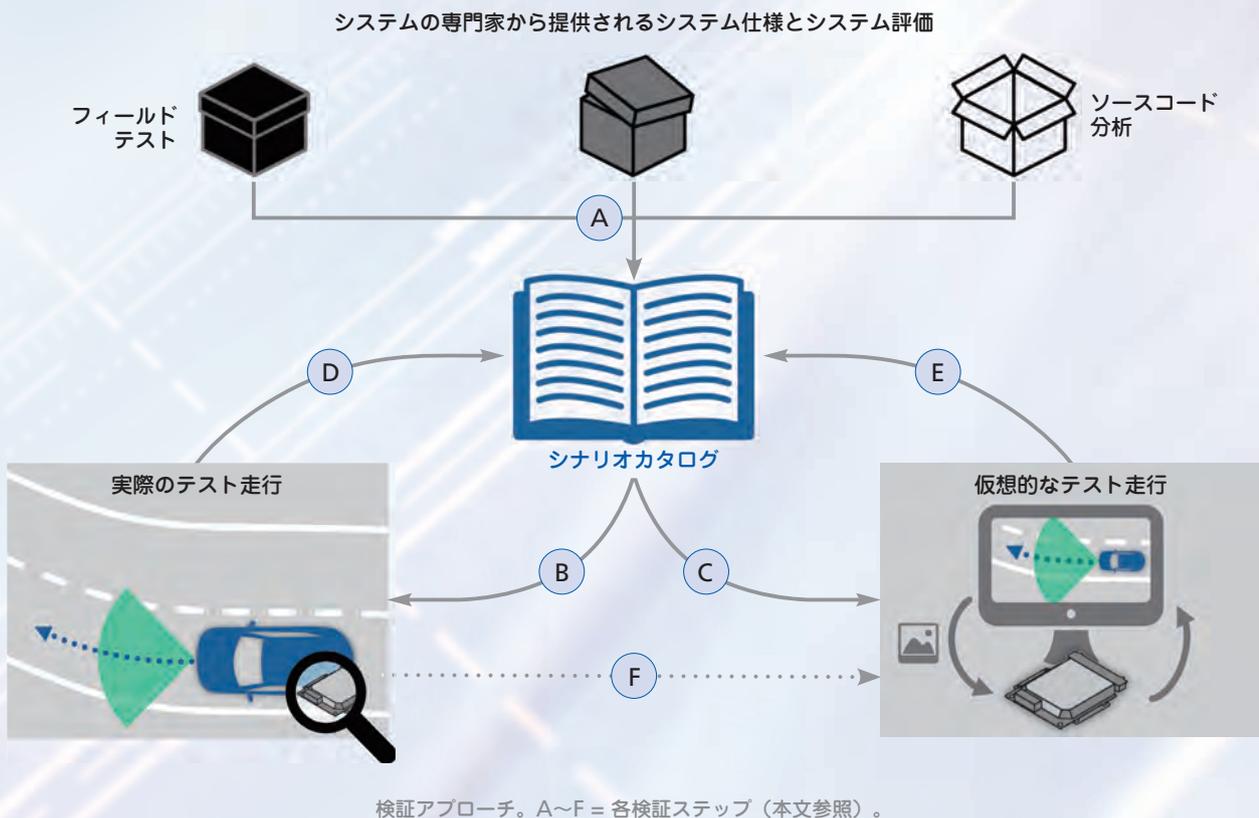
*今後サポート予定

Robust Assistance Systems

ロバストな運転支援システム

反復検証のための戦略

ソフトウェアで制御する自律走行車には「検証」が不可欠です。これを効率的に行うにはどのようにすればよいでしょうか。事前に策定されるシステム仕様において実際の交通状況で起こりうるすべての事態を考慮することは不可能なので、それを補うソフトウェアシステムの「ロバスト性」が強く求められることとなります。この「ロバスト性」は、拡張可能なシナリオ形式のカタログに基づくテストを仮想環境において反復実行することによって実現することができます。



自動運転の車両ではドライバーに時間の余裕が生まれます。あなたならその時間をどのように過ごしますか？書類整理をしたり、オンラインショッピングをしたり、のんびりくつろいだりと、可能性は無限です。しかしこのようにドライバーが両手をハンドルから離して快適に過ご

せるようになるには、自動運転の技術が全面的に信頼できるものでなければなりません。

そのためには、機能レベルのシステム障害に対応するISO 26262 準拠のアクティブ支援システムを装備するだけでは足りません。全自動運転に安全策を組み

込み、現在の状況が誤って解釈されることが絶対にならないようにする必要があります。しかしここで障害になるのは、交通や天候、光の条件など、システム仕様に影響を与える要因があまりに多く、すべての事態に対応することができないということです。

先進運転支援システム (ADAS) の分野では、この障害は「機能的不備 (functional insufficiency)」と呼ばれており、これを解決するのがソフトウェアの「ロバスト性」です。「ロバスト性」とは、どのような異常事態においても定義されたとおりに機能して適切に対処できることを意味します。全自動運転の実現のためには、不完全な仕様に基づいて工程を進めなければならない場合でも、ソフトウェア制御式運転支援システムのロバスト性を社会的に認められるレベルまで引き上げなければなりません。つまり、可能な限り実際のアプローチを採用して安全なシステムを作り上げる必要があるのです。

等価クラスに基づくシナリオ記述

最近の技術研究論文には、前述のような課題の重要性を明確に示すものが多くみられます。たとえば、ドイツのダルムシュタットを拠点としている Hermann Winner 教授は、確率に基づく自動運転車用の検証アプローチを発表しています。教授の研究によれば、運転支援システムを搭載していない車両が起こす負傷事故件数を半分に抑えるための知識や技術を確立するには、比較的単純なユースケースであっても、テスト車両を 2.4×10^8 キロメートル走行させる必要があります。このような検証の目的は、システムがメトリック (品質の測定基準) M を達成する確率 P を示すことにありますが、たとえばテストサイトが「ハイウェイ」 ($d_e = \text{highway}$) である場合の達成確率は、 $P(M | \text{highway})$ によって求められます。

ハイウェイ以外でのシステム挙動を調べる場合は、テストサイトは「非ハイウェイ」 ($d_e = \text{non-highway}$) となるので、このメトリックを達成する全確率は $P_{\text{tot}}(M) = P(M | \text{highway}) \cdot P(\text{highway}) + P(M | \text{non-highway}) \cdot P(\text{non-highway})$ となります。テスト走行の結果、ハイウェイ以外のサイトをさらに都市部と地方部に分けなければならないような場合もありますが、特定の地域において被験システムが等価的に挙動するのであれば、 $d_e = \{\text{highway, urban,}$

$\text{rural areas}\}$ というようにテストサイトを3つの等価クラスに分けることができます。

また、乾いた路面で完璧に機能していたシステムが濡れた路面では正しく機能しなくなる、といったことはよくあることですが、そのような問題をシナリオの記述に反映させるには、さらなる特性として道路状態 $d_s = \{\text{dry, wet}\}$ を定義します。その結果、6つのシナリオでメトリックをテストすることになります。

一般に、シナリオ S は $S = [d_1, d_2, \dots, d_n]$ のように、各等価クラスと各特性の組み合わせとして定義することができます。メトリックを達成する全確率

$$P_{\text{tot}}(M) = \sum P(M | S_i) \cdot P(S_i)$$

は、一般的には n 個の特性 d_n について計算されます。ここで、シナリオ数 i はすべての特性の等価クラスのカーディナリティ (分散度) を掛け合わせたもので、 $i = \prod |d_n|$ という式で求められます。

実験では、 $P(M | S_i)$ を明確にするための具体的なテストケースが必要です。テストケースが1つのシナリオを表すので、各種シナリオの総数がテストケース数の基準値となり、確実なシステム検証を行うにはこの値が極めて重要なものとなります。

シナリオの反復的拡張

シナリオの記述は、等価クラスに基づいて作成した後に反復型手法によって改良を重ねることにより、自律システムを検証するためのアプリケーションベースの工程に適用できるようになります。この工程は左図に示すとおりです。

この反復型検証戦略の中核となるのは、以下の3つのソース (図中の A) から導かれた情報に基づく「シナリオカタログ」です。

- (1) システム挙動が期待どおりではなかった耐久テストとフィールドテストの結果
- (2) システムの専門家から提供されたシステム仕様とシステム評価に基づいて作成されたシナリオ
- (3) 静的ソースコード解析から生成されたシナリオ

このシナリオカタログは、実際のテスト

走行の体系化 (B) に使用されるだけでなく、仮想テスト走行のパラメータ設定 (C) にも役立ちます。仮想テスト走行のメリットとしては、高価なテスト車両の可用性に依存することなく任意の台数のコンピュータ上でテスト走行を同時に行うことができる、また実際のテストドライブで発生する危機的な状況を仮想的に再現し、必要に応じて修正を加えることができる、といったことがあります。テスト走行で得られた結果から新しいシナリオを作成し、それらを解析してカタログに追加することができます (D、E)。この繰り返しにより、テストのカバレッジが継続的に向上していきます。

運転支援システム全体の各領域をまたがるシミュレーションの検証を行うには、現実と仮想のテスト走行を比較することにより基礎モデルを検証しておくこと (F) が欠かせません。この比較を行うことによってのみ、各モデルだけでなくすべてのシミュレーションの精密さに関して信頼できる記述を行うことが可能になります。しかもこの工程では、運転支援システムの仮想テストを行うための基礎が形成され、次第に包括的かつ正確なものになっていきます。このように仮想テストは、テストの費用と時間、さらには管理工数も抑えながら品質を高めていくための重要な手段になり得るのです。

執筆者

Marius Feilhauer
ETAS GmbH

テスト・評価事業部
運転支援システム用
シミュレーションモデルの
開発責任者

Dr. Jürgen Häring
ETAS GmbH

テスト・評価事業部、
製品管理部門長



ETAS INCA-RDE

執筆者

Dr. Ulrich Lauff
ETAS GmbH
 マーケティング
 コミュニケーション
 上級エキスパート

Rajesh Reddy
ETAS GmbH
 プロダクトマネージャ
 INCA-RDE ツール担当

車両の排ガスを実際の運転条件下で測定

2017年以降、EU諸国で登録される車両はすべて実路走行排気（RDE）の検査を受けなければならないとなりましたが、ETASが開発したテストドライバー向けアシスタントソフトウェアを使用すれば、テストドライバーが測定値をリアルタイムに追跡し、RDEデータが法定限度内に収まっているかを監視することができます。このソフトウェアはETAS INCAにシームレスに統合されているので、いつもの手慣れた計測/適合環境でRDE試験を行うことができます。つまり、制御された再現可能な手法によるRDE運転試験の実施が実現できるのです。

排ガス規制に対応するには、測定値収集のための運転時間、都会/地方/高速道路における所定の走行距離、許容される速度範囲、運転性能に関する諸要件など、多くのパラメータを考慮しなければなりません。テストや適合を担当するエンジニアには、最新の排ガス測定データも必要です。

INCA-RDE

ETASは、このRDEアシスタントをINCAのアドオン製品「INCA-RDE」として発売する予定です。この製品で、運転試験中に測定データをリアルタイムに評価することができます（図1を参照）。INCA-RDEは、INCAで実験を行うドライバーに対して、以下の情報を専用の仮想インストゥルメント（画面上の仮想計器）に表示します。

- GPSの位置データ
 - 排ガス測定の開始
 - 測定結果
 - 測定装置の監視
- さらに、以下のテストパラメータも表示します。
- 環境条件とエンジンの状態
 - ルート区別の走行距離と走行時間
 - 車両の速度と加速度
 - 測定値のRDE要件適合性の評価

図2は、INCAでの実験中に収集されたRDEデータの表示例を示しています。

運転モード

INCA-RDEソフトウェアツールは、CANプロトコルによりES59xインターフェースモジュール経由でPEMS（車載型排ガス計測システム）ハードウェアに接続します。INCA-RDEは排ガス測定データをオンラインで評価するだけでなく、PEMSで収集されたOBDデータとGPSデータも同様に評価します。これに関連し、「移動平均法（EMROAD）」と「性能クラス別評価（CLEAR）」という2つの手法を用いて車両のダイナミクス状態を確認できます。分析結果、つまり実際のRDEデータは、INCAの実験ウィンドウ内のRDE専用インストールメントに表示されます。このデータは、ECU（エンジン制御装置）からの測定信号と同期して10ミリ秒ごとに記録されるので、測定完了後は、記録されたRDEデータとECU信号とを簡単に同期させて分析することができます。

まとめ

INCA-RDEを使用することによりテストエンジニアは、試験走行中に収集されるRDEデータの状態を、視認性のよい専用インストールメントでリアルタイムに把握することができます。このソリューションは、車両データの記録、ECUパラメータの適合、診断データの評価などを行うINCAの環境に統合されているので、RDEの排出量を効率的に測定し、所定のECU信号とともにこの排ガスデータを分析することが可能になります。

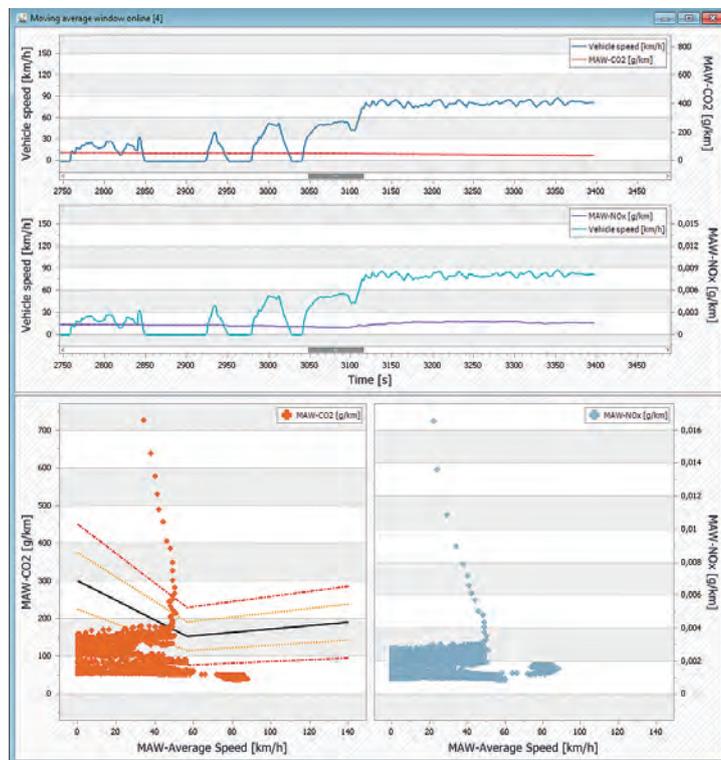
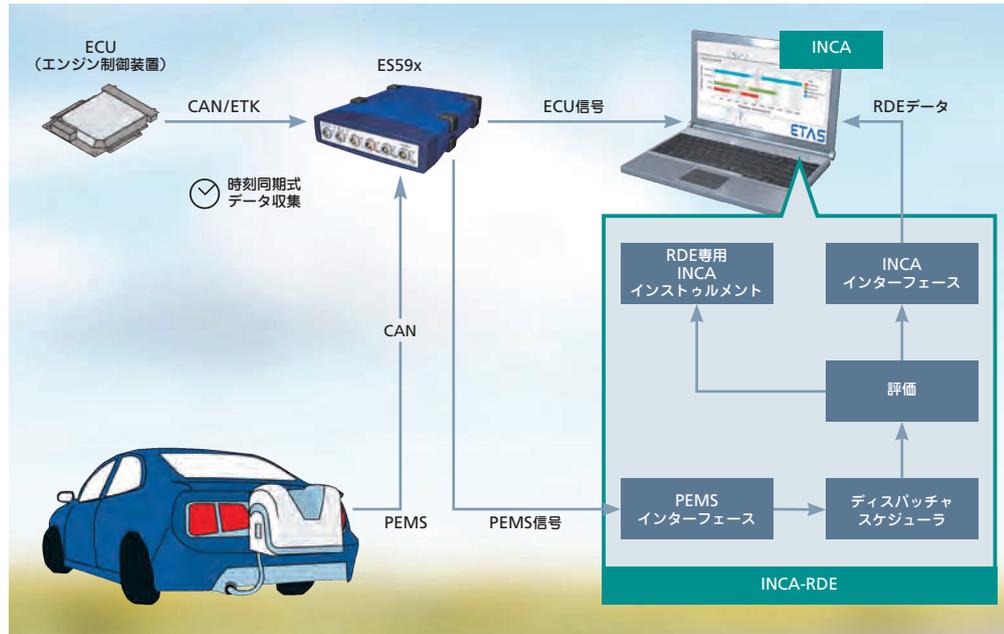
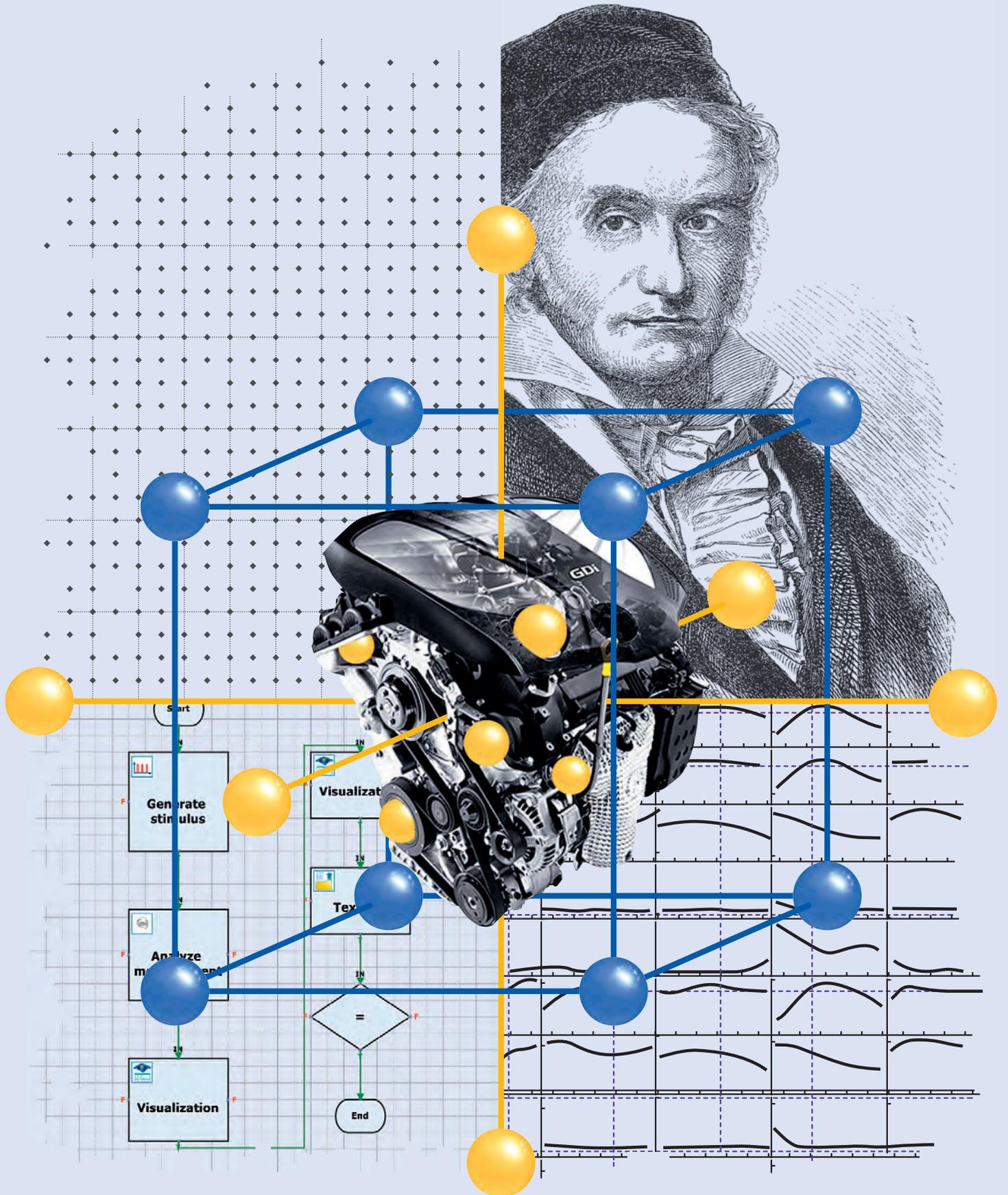


図2: 上の2つのグラフー測定時間(秒)の経過に沿った車速とCO₂/NO_x排出量(g/km)、下の2つのグラフー車速(移動平均)に対するCO₂/NO_x排出量。左下のグラフは、テスト車両のCO₂特性カーブ(黒色の線)とその許容範囲(黄色と赤色の線)を示しています。RDE試験では、移動平均ウィンドウ(MAW)内に表示されるCO₂平均値の半分が、内側の許容値範囲内に収まらなければなりません。

図1: システムの概要
排ガスは、テスト走行においてポータブルな測定装置で測定され、INCA-RDEにより評価された結果がINCA上の専用インストールメントにリアルタイムで表示されます。



Optimization of Gasoline Engines

ガソリンエンジンの最適化

Hyundai におけるモデルベース適合

Hyundai Motor Company (HMC) では、性能、燃費、汚染物質排出量に関する厳しい要求に応えるため、より効率的なエンジンとシステムの開発を進めています。多数の制御系により実現される「多自由度」は、非常に多くの「パラメータ」として実装され、これらのパラメータは、適合工程において調整し、最適化する必要があります。

韓国の南陽にある Hyundai Motor Company (HMC) 研究開発センターは、エンジンの動作範囲全体にわたる適合を効率的に行うことのできる「モデルベース適合」の工程を新たに導入しました。この新しい工程では、ETAS ASCMO および ETAS INCA-FLOW というソフトウェアツールによる高度なモデリングと自動化の手法を用いています。Hyundai

はこの新しい工程を導入することにより、ガソリンエンジン用の従来の標準的な適合工程に比べて計測工数を 75 パーセントも低減することに成功し、同時に品質向上も実現できました。

プロジェクトの概要

Hyundai では、新しい工程によって低減できた計測工数を算出し、ガソリンエ

ンジン用の標準的な適合パッケージに基づく成果物の品質を分析しました。ここで使用されたエンジンは、3 ステージ吸気装置搭載、デュアル連続可変バルブタイミング機構採用で、Continental エンジン制御装置により制御された自然吸気式の V6 3.0L GDI エンジンでした。各適合値（吸排気カムシャフトタイミング、噴射タイミング、点火角）を最適化し、

執筆者

Yooshin Cho 氏
Hyundai R&D
Center

(韓国、南陽)
上級エンジニア
ガソリンエンジン試験方法
の担当者

Wonseok Chang、
Wongun Yoo
ETAS Korea
Co. Ltd.

フィールドアプリケーション
エンジニア

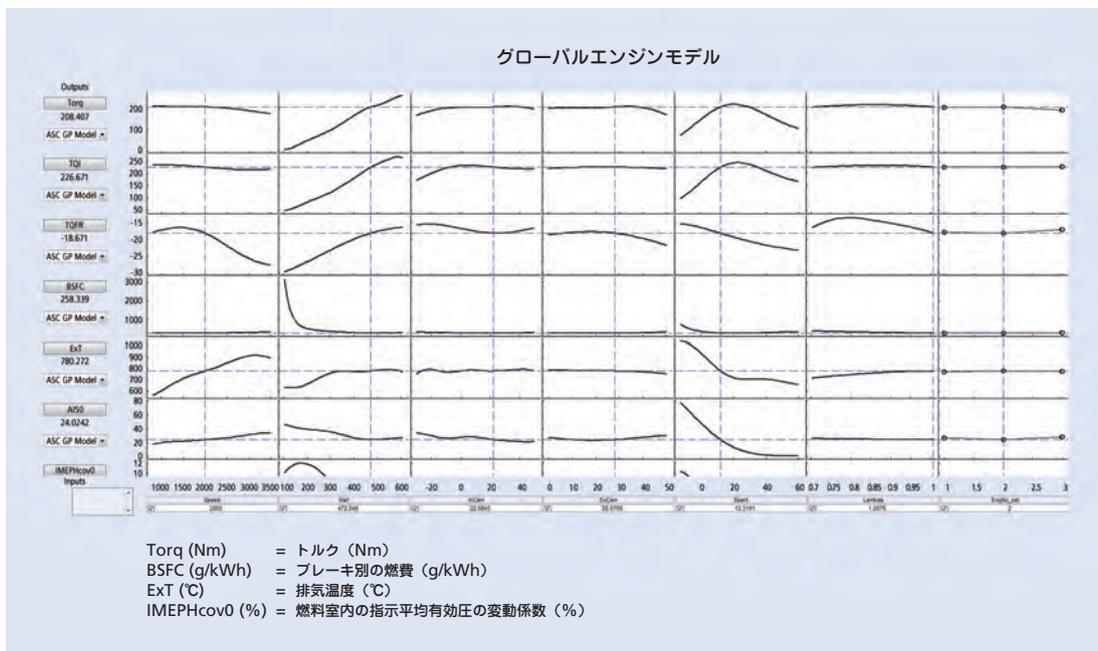


図 1: 出力変数と入力変数の依存関係を示すグラフ。ETAS ASCMO モデルは、この依存関係をパラメータ空間全体にわたって非常に的確にシミュレートします。

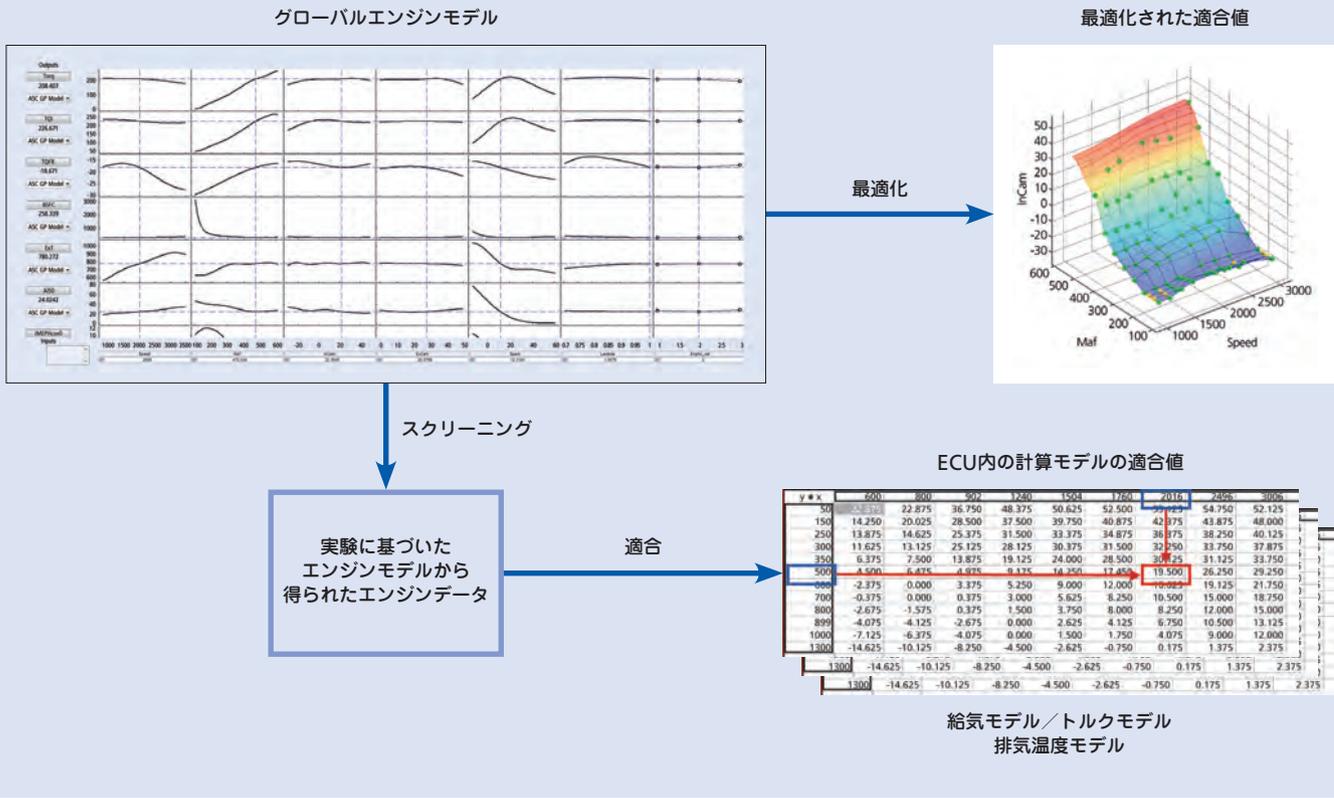


図 2: ECU 内のモデルのパラメータ値の最適化 (「最適化機能」)
- 各モデルの出力を、実験に基づいたエンジンモデルから ASCMO が「スクリーニング」によって導出したデータに合わせて調整 (「適合」) する。

各 ECU モデル (給気、トルク、排気温度) の適合も行いました。

新しい適合工程

Hyundai では、適合工程を再構築する過程において、「実験計画法」(DoE)と「完全自動計測」という 2 つの新しい手法をエンジンダイナモメータに実装し、機械学習の技術と計測結果から、エンジンの挙動を正確にシミュレートする高度なモデルを開発しました。DoE (実験計画) とモデルは ETAS ASCMO ツールにより生成され、DoE に基づくテストポイント計測は、ダイナモメータのテストセルにおいて、INCA-FLOW ツールで新たに開発した計測制御システムにより自動化されました。

エンジンモデルを用いた適合

テストベンチで計測された値から生成されたエンジンモデルは、エンジンの挙動をパラメータ空間全域にわたって高い精度でシミュレートします (図 1 を参照)。このモデルに基づいて、燃費と全負荷ト

ルクの双方が最適化され (図 2 を参照)、同時にノッキング限界と排気温度限界が確認されました。一般的に、給気、トルク、排気温度などの ECU モデルを適合するには大量のデータが必要ですが、ここで使用されたデータは、従来の一般的な手法のようにエンジンダイナモメータにおいて手間をかけて計測したのではなく、実験に基づいたエンジンモデルから ASCMO が「スクリーニング」と呼ばれる手法で導き出したものでした。ASCMO が生成したモデルの出力値を実測値と比較した誤差は、給気モデルでは 5% 未満、トルクモデルでは 5% 未満 (または最大 5 Nm)、排気温度モデルでは 15°C 未満でした。

結論とまとめ

Hyundai では、グローバルなモデルベース工程を導入したことでエンジン適合の効率を劇的に高めることができ、エンジンダイナモメータでの計測工数を従来の手法に比べて 75% 低減することができました。以上のことから同社は、グロー

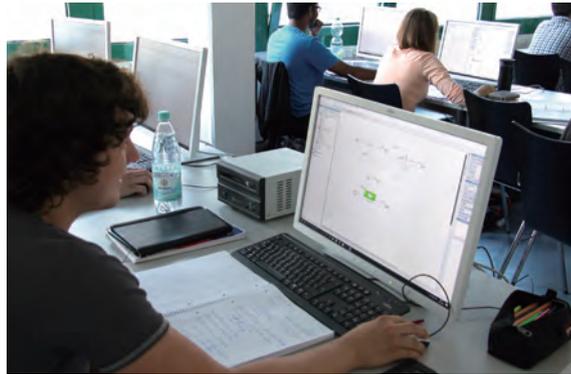
バルなモデルベース工程は複雑なエンジンの適合を効率化し、プロジェクトの設定目標に対して高品質の成果をもたらすことができるものと結論付けました。

ASCET at the University Lab

大学のラボで ASCET を体験

シュトゥットガルト大学においてモデルベースのソフトウェア開発のセミナーを開催

ETAS とシュトゥットガルト大学との緊密な協力関係の一環として、ETAS の常駐エンジニアである Andy Staats と Christoph Schlegel が「自動車ソフトウェアのモデルベース開発」という演題のセミナーを開催しています。このコースを受講する学生たちは、ECU のプログラミングに使用されるソフトウェアアーキテクチャや手法について実践的に学ぶことができます。ここで特に焦点が当てられている「モデルベース開発」という手法は、抽象化による再利用性や品質向上を実現できるという理由で自動車産業界のソフトウェア開発に好んで用いられているものです。コースの中心となるのはコンピュータラボでの実践練習で、ECU ソフトウェア開発の手法に重点を置いたものが行われます。学生たちは ETAS ASCET で ECU ファンクションのモデリングを行い、そのモデルを ETAS ES910 プロトタイピング/インターフェースハードウェアなどのラビットプロトタイピングハードウェアでテストします。「ETAS の ASCET ラボで小グループに分かれ多くの問題をこなしていくことは、とても有益です。学習した知識とスキルを応用すること



シュトゥットガルト大学の ASCET ラボでは、学生たちがソフトウェア開発を通じて実践的な経験を積み重ねる機会を得ることができます。

ができ、ミスから学ぶこともできるからです」と Andy Staats は語り、さらに次のように力説します - 「学生たちにとっての一番のメリットは、自動車産業界で実際に使用されている手法やソフトウェアとハードウェアについて習熟できることです」。これは「理論と実践」の組み合わせが有意義であることを示すよい一例といえるでしょう。

Students Develop Autonomous Race Cars

学生たちが自動運転のレースカーを開発

ETAS が未来技術の実践経験を支援

学生フォーミュラドイツ大会は、学生が自動車産業界における開発の過程を実際に経験できる絶好の機会です。自動車産業界で活躍するには、燃焼機関や電気エンジンといった技術の専門知識が必要となります。自動運転の時代となった今日、学生は自動運転技術に関する知識も確実に身につける必要があります。このような理由から、学生フォーミュラは今年度から新たに Formula Student Driverless (FSD) という自動運転のフォーミュラカーレース大会を立ち上げました。この大会では分野を横断したコラボレーションに重点が置かれ、自動車技術や電気工学の分野の学生たちがコンピュータサイエンス、データ処理、センサ技術を専攻する学生たちと協力して、FSD で規定される要件を満たすレースカーを開発します。

学生フォーミュラ参加チームのスポンサーを長年務めている ETAS は、2017 年から FSD の後援も行っていきます。チームは年間を通して、特にシーズン中は ETAS から各種製品や専門家によるテクニカルサポート、そして金銭面でのサポートを受け



ることができます。このため、参加する学生たちは技術的な専門知識を身に付けるだけでなく、卒業前に ETAS 製品を経験する機会を得られます。その結果として、彼らは FSD 競技においても、また将来のキャリアにおいても、有利な位置に立つことができます。

KA-Racing
Driver-less 2017
(カールスルーエ
工科大学)

Fascinating ETAS Measurement Technology

ETAS の魅力的な計測技術

実習生たちが実習でテスト車両を構築

実習生たちが計測技術を明快かつ実践的に身につける手段はないでしょうか。ドイツのシュヴィーバーディンゲンにある Bosch の職業訓練部門が ETAS に投げかけたこの質問に対する答えは、「ETAS デモカーの構築」でした。

執筆者

Klaus Fronius
ETAS GmbH

ユニバーシティリエゾン
 マネージャ



車内を埋めつくすノート PC やケーブルの絡まりが解消されつつあることを見て取ることもできます。

ETAS デモカーのこの海外ツアーは、最終目的地に向かう途中の寄り道に過ぎません。今後は、将来を担う若手の計測／適合エンジニアが車両を対象に行うべき複雑な業務を学ぶうえでこの ETAS デモカーは、最新の ETAS ツールを備えたよき「教材」となることでしょう。これは「最適なトレーニングを行うには、最新設備が整った安全な作業場が必要である」という強い信念に基づいています。このように、単科大学や総合大学との力強いコラボレーションは、ETAS の事業戦略に不可欠なものとなっています。

ETAS デモカーは
 エンベデッドワールド 2017
 で注目を集めました。

どこにでもある普通のプラグインハイブリッド車がわずか数カ月で、ハイテク機器の内装を施したインパクトのある車に変貌しました。室内にはさまざまな ETAS の計測用ハードウェア (ES4xx、ES5xx、ES6xx、ES9xx、さらに新しい ES8xx シリーズ) が組み込まれています。しかし、こうしたハードウェアもソフトウェアがなければ何もできません。そこで、第 1 段階として ETAS INCA-TOUCH がこの車に組み込まれました。このソフトウェアは内蔵タッチモニターで操作でき、INCA のボイスコマンドを用

いて機能を制御することもできます。そして第 2 段階では、技術者や実習生のための実践的なトレーニングとして、より手の込んだ変貌が遂げられました。スタイリッシュな ETAS デモカーは、この数カ月間、ヨーロッパ各地の展示会やイノベーションイベントで多くの注目を集めました。フランスやベルギー、イタリア、英国のほか、ドイツのニュルンベルクで開催されたエンベデッドワールド 2017 でも、このデモカーに高い関心が寄せられました。改装されたこの車両で計測技術を実際に経験することができ、

Measuring and Calibrating During Test Drives

テスト走行中の計測／適合

ETAS INCA-TOUCH で INCA の実験を安全かつ確実に表示して操作する

テスト走行中のノート PC の使用は、安全性のリスクが高まるため、禁止する企業が増えてきています。しかし、それでもエンジニアは計測を行い、車両ファンクションの挙動を検証して適合しなければなりません。そのような場合、INCA-TOUCH インターフェースを使用すれば、タッチスクリーンやボイスコマンドでより安全に ETAS INCA を操作することができます。

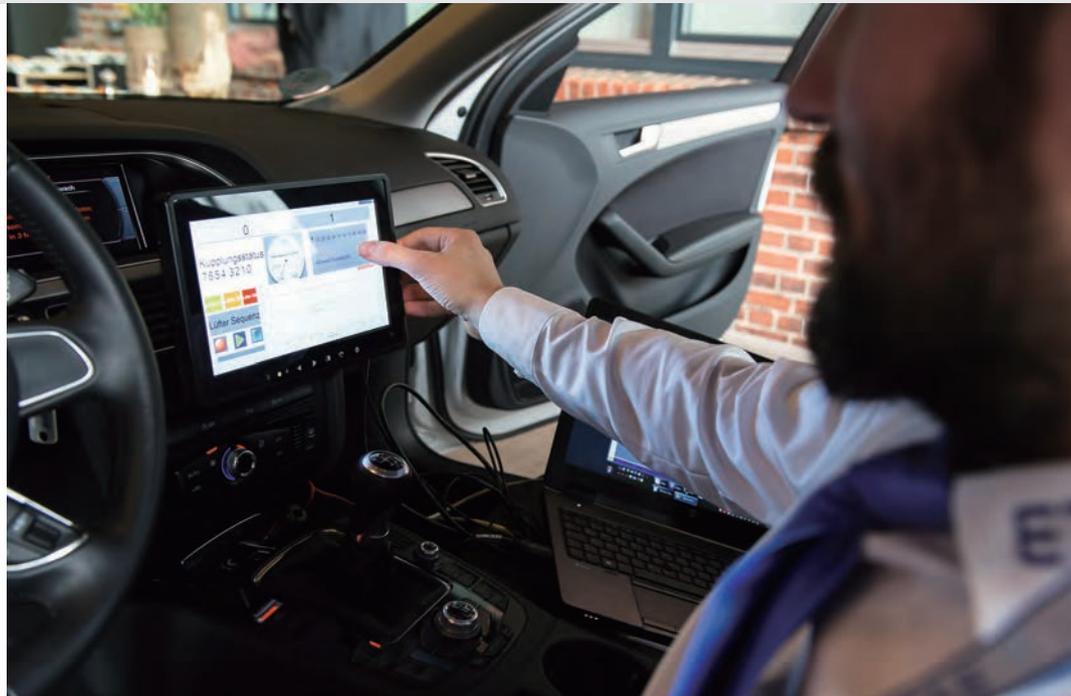
タッチ操作

INCA の主な計測／適合機能は、INCA-TOUCH から操作できます。タッチスクリーン向けに最適化された視認性のよい「仮想計器」を利用して、「測定変数」の値を読み取ったり、「適合変数」（ECU パラメータ）の値を変更したりすることができます。これらの計器は、ノート PC を INCA 用に使用する場合は PC に接続したタッチスクリーンに表示でき、Windows タブレットを INCA 用に使用する場合は、タブレットのディスプレイに直接表示することができます。

主な特長

セキュアで安全、しかも使いやすい

- 操作機能：計測の開始／終了／一時停止、データ記録、記録開始トリガ発行、ハードウェア初期化など
- 測定値をさまざまな「仮想計器」（オシロスコープ、棒グラフ、テーブル、ビット表示、カーブ／マップ、回転計、LED など）に表示
- 画面上のコンテンツを複数の「レイヤ」に分類して割り当てることで、多くの変数を目的別に表示することが可能



自動化のための機能

- ステップごとに定義された個々の適合操作を、タッチボタンのタップ操作により実行
- 一連の適合手順を、変更可能な反復区間やダイアログボックスとともに定義
- 別の実験シナリオへの切り替え

INCA をさらに使いやすい補助機能

- 実験の制御や ECU パラメータの適合をボイスコマンドで操作
- データ記録中にマーカーをデータとして挿入。オプションにより音声コメントの付加も可能。

INCA-TOUCH は、内蔵タッチモニターによる操作も可能（上の写真を参照）

Learning About Assistance Systems in Bavaria

バイエルンで 支援システムを学習

ETAS がケンブテン応用科学大学の「A ドライブリビングラボ」をサポート

ドイツ・バイエルン州南部のアルゴイ地方にあるケンブテン大学は、世界唯一の運転支援システム修士課程の設立によって大きな変革を遂げました。世界中の学生がこのラボに参加しようと列をなし、OEM やサプライヤもこの新しい「A ドライブリビングラボ」への参入に意欲的です。今回のインタビューでは、コーディネータの Stefan-Alexander Schneider 教授に、このラボの全容について、またそこでの ETAS と ETAS ISOLAR-EVE の役割について説明していただきました。



インタビュー

Prof. Dr. Stefan-Alexander Schneider
ケンブテン応用科学大学
(ドイツ)

運転支援システム
修士課程の責任者

RealTimes：アルゴイと自動運転と支援システム、これらはどのようにつながるのでしょうか。

Schneider 教授：ここケンブテン大学には、世界で唯一の運転支援システム修士課程があります。この課程には3つの学部在籍する教授15名の経験が生かされています。その中で指導的役割を担っているのが私の自動運転・支援システムコースの講座で、このコースは2013年末までに、5年間にわたり Continental から基金の寄付を受けました。この業界には支援システムの開発手法に精通したシステムエンジニアに対する大きな需要があり、そのようなエンジニアを私たちは2014年から養成しています。世界中の大学志願者たちが本学への入学を希望し、応募してきています。そして本学のトレーニングの実用性を最大限に高めるため、私たちはこのたび「A ドライブリビングラボ」を始動させました。

RealTimes：このラボはどのようなものなのでしょうか。

Schneider 教授：私たちは、支援システム開発のための「価値創生チェーン」の全体を再現する500m²のエリアを設け、必須の工程や手法、ツールなどについて「開発前」の状態から学生に教示しています。ここには開発工程を分析して最適化することも含まれます。電気工学

や機械工学、さらにIT分野が密接に連携して関与し、それぞれの専門知識が生かされています。

RealTimes：「A ドライブリビングラボ」の「A」は何を表しているのですか。

Schneider 教授：まさにあなたが冒頭におっしゃった3つのもの – アルゴイ (Allgäu)、支援システム (Assistance Systems)、自動運転 (Autonomous Driving) – を表しています。ですが、このラボはソフトウェアやシステムの開発に使用されているVモデルに基づいているので、「Vラボ」でもよかったですかもしれません。ラボは50×10メートルの細長いV字型になっていて、要求分析から始まり、機能仕様やシステム仕様の策定から各種検証までの各ステップがそれぞれ「ステーション」として順に並んでいます。実際の開発工程を再現したオールインワンの環境において学生たちは、知識や技能を身に付け、研究を行えるのです。ここではETASからの支援を受けており、仮想ECUを生成するためのISOLAR-EVEや、ハードウェアインザループシステムのETAS LABCAR、オープンソースソフトウェアのBUSMASTERなどのプロ用ツールを提供していただいています。このようにして本学の学生たちは、将来の職場で使用することになるツールチェーンに慣れ親しむことができるのです。



RealTimes：仮想 ECU の応用分野として、どのようなものを思い描いていらっしゃいますか。

Schneider 教授：そうですね、1 つ実現したいと考えているのは、さまざまなドメインの ECU を接続することです。運転支援システムの場合、パワートレイン ECU やシャーシ ECU と環境認識・監視用センサシステムとの相互作用が重要です。特に重要な要素となるのは、カメラやレーダー、ライダーシステムと仮想 ECU との協調シミュレーションや、仮想 ECU ネットワーク内での協調シミュレーションですが、これを実現するには、システム間の相互作用や車両内のリアルタイムデータ通信について理解を深め、最終的には車両とインフラストラク

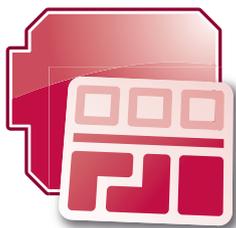
チャとの通信をさらに深く理解することが必要です。このような場面において「仮想化」は非常に便利な手法であるといえます。また当然ながら、私たちは常に現行の開発手法を進化させていく必要があり、昨今では、新しいファンクションを後から追加できるような「アジャイルソフトウェア」の開発がトレンドとなっています。さらに、このような柔軟性が求められている反面、各ファンクションの適切な評価と検証も欠かせないものとなっています。これらのトピックはこの業界における重大な関心事となっており、そのことは、「A ドライブプリングラボ」設立直後からさまざまな EM や Tier 1、Tier 2 サプライヤにご参加いただいているという事実にも現れてい

ます。今後数カ月間でインフラストラクチャの準備が完全に整い、私たちは本格的に始動できる予定です。



ISOLAR-EVEでADAS ECUを仮想化

ISOLAR-EVE ツールは、ECU アーキテクチャのすべてのコンポーネントを含めた実 ECU の挙動を PC 上できわめて現実的にシミュレートすることができるので、ADAS ECU の仮想化を行うのに最適です。仮想化 ECU には、完全な AUTOSAR OS とともに基本ソフトウェアとアプリケーションソフトウェアがすべて実装されます。また、マルチコア構成を現実的にモデリングして、異なる複数のマイクロコントローラやマイクロプロセッサで構成されるヘテロジニアスなアーキテクチャを提示することもできます。このように ISOLAR-EVE ツールは、複数のコネクテッド ECU とそれらの相互通信のシミュレーションを強力にサポートします。



詳しい情報はこちら：
www.etas.com/isolarb

ETAS ISOLAR-B Completes the AUTOSAR Tool Chain

ETAS ISOLAR-B で完成する AUTOSAR ツールチェーン

ISOLAR-B は AUTOSAR 準拠の基本ソフトウェアを設定するツールで、ECU の統合を担当する「ECU インテグレータ」を多くのルーチン作業から解放し、ゆとりを生み出します。明確な情報表示や、反復的開発フローのサポート、高度な自動化、早期検証、といった機能により、目標到達までの時間を短縮し、品質も高めることができます。システム情報をインテリジェントに評価できるので、ECU

インテグレータは接続や関係性をより素早く把握することができます。システムエクステンションを使用すれば、システムディスクリプションと基本ソフトウェアコンフィギュレーションとの間の隔たりを埋めることができ、設定作業を軽減できます。ISOLAR-A や RTA-BSW (基本ソフトウェア) との併用で、シームレスに調和シラバンスのとれた AUTOSAR ソリューションを実現でき、その効果は

すでに数々のプロジェクトで実証されています。ISOLAR-A と ISOLAR-B は AUTOSAR のリリース R4.3 をサポートし、共有データベースを使用します。これにより、ラウンドトリップタイムの短縮や、設定の簡素化とさらなる自動化を望めるので、生産用プロジェクトの効率も大幅に向上します。ISOLAR-B は Eclipse プラットフォームを採用し、既存の Eclipse 開発環境への統合も容易です。

New ES300 Series Measurement Module

新しい計測用ハードウェア ES300 シリーズ

ETAS ES300 シリーズの
 モジュール同士は
 容易に接続可能



2017 年、ETAS の計測ツール群は、小型でコストパフォーマンスに優れた計測モジュール「ES300 シリーズ」を新たに迎え、さらに拡充されました。防水防塵構造のため、テスト車両のエンジンルームやシャーシに設置して使用することができます。このモジュールで計測したデータは共有の CAN バス経由で転送できるので、ES582 や ES584 などの USB CAN インターフェースモジュール経由で INCA に接続することにより、ECU からの CAN 信号と同期して収集することができます。現在、8 チャンネルの ES321 温度測定モジュール、4 チャンネルの ES313 A/D モジュール、4 チャンネルの ES341 デジタル入力モジュールが販売されています。ES313 と ES341 は、センサに供給するための電源が各チャンネルに装備されています。



Better Scalability for Test Systems

テストシステムの 拡張性を向上

LABCAR HiL テストシステムの拡張性を高めるために ETAS が開発してきた多種多様なシステムコンポーネントは、多くのユーザープロジェクトで活用されています。これらを用いて、独自の ECU テストシステムを構成したり HiL テストベンチをフレキシブルに構築したりすることができ、システムや車両全体の検証に役立てることができます。

中心的なモジュール群となるのは、19 インチラックに格納できる PCI-Express ES5300 プラットフォームとそのプラグインボードで、ラックの幅は 60 または

80 cm、高さは 24、33、38 U のものがあります。80 cm 幅のラックにはカバー付き開口部が最大 24 か所設けられており、各種部品（最大 300 ピンの高密度 ECU コネクタ、バスインターフェースコネクタ、ヒューズホルダなど）用のプレートを取り付けることができます。内部配線は側面内部に取り付けられているパネルに沿って、最適な長さで設置することができます。必要に応じて、信号経路の切り替えスイッチや、スタンバイ電流などの供給電流や負荷電流を高精度で測定するモジュールなどを取り付けることもできます。

これらのコンポーネントで構成される LABCAR システムは、電磁環境適合性 (EMC) に関する IEC 61326-1 規格に準拠しています。ES53xx I/O モジュールの回路基板レイアウトは、閉ループテストの信号遅延を最小限に抑えることはもちろん、EMC についても慎重に考慮して設計されています。納入されるシステムは安全規格 IEC 61010-1 に準拠したものとなっており、難燃性部品の使用や、機械的保護テストや静電放電 (ESD) 保護テストの実施、といった対策が施されています。

新しいドライブレコーダ - ES820



New ES820 Drive Recorder

新しい ドライブレコーダ - ES820

2017 年 9 月に発売された ETAS ES800 システムのひとつである ES820 ドライブレコーダは、INCA (PC) の代わりにデータの計測と記録を行うハードウェアモジュールで、車両電子システムの開発、適合、検証などの工程における各種計測作業に利用することができます。ES89x

シリーズや ES5xx シリーズのインターフェースモジュールとの併用で、各種 ETK (ETK、XETK、高性能 FETK) や複数の車載バス (LIN、CAN/CAN FD、FlexRay) を経由して ECU をドライブレコーダに接続することができ、ES400 シリーズや ES600 シリーズの計測モ

ジュールと併用すれば、車両の各種センサ信号なども高速で取得することができます。計測データの記録には、記憶容量 128 GB の内蔵ソリッドステートドライブ (SSD) のほか、交換が容易な SSD メモリモジュール (500 GB または 1 TB) も使用することができます。

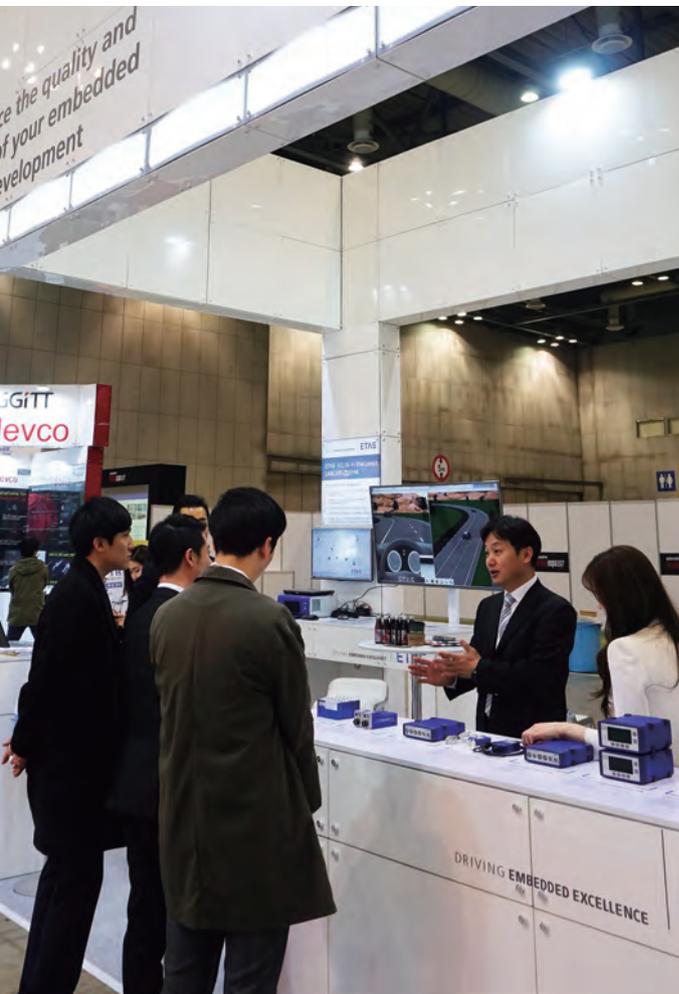
ETAS ブラジル法人は、サンパウロで開催された International Symposium of Automotive Engineering (SIMEA) に参加しました。主要テーマ：机上からネットワークシステムまで拡張可能なテスト、計測ツール



One Year in ETAS Pictures

写真で振り返る ETAS の 1 年

ETAS 韓国法人は、ソウルで開催された Automotive Testing Expo 2017 でソリューションを発表しました。主要テーマ：XiL (X インザグループ)、すべての計測ソリューション



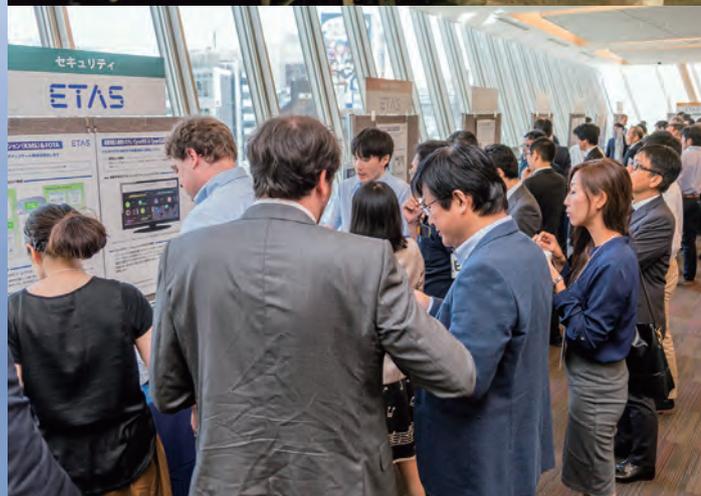
ETAS と ESCRYP T は、ドイツのニュルンベルクで開催されたエンベデッドワールドで、ソフトウェア開発や安全とセキュリティに関するソリューションを発表しました。INCA-TOUCH と ETAS ハードウェアを搭載した ETAS デモカーが注目を集めました。





ドイツのシュトゥットガルトで開催された Automotive Testing Expo 2017 の ETAS ブース。机上からネットワークシステムまで拡張可能なテスト、計測、検証がフォーカスされました。

ETAS 日本法人は、2017 年 9 月 29 日、東京にて第 9 回目の車載制御・組み込みシステム開発シンポジウム 2017 - Symposium on Automotive Embedded Systems Development 2017 を開催し、約 420 名のお客様にご来場いただきました。



ETAS 英国法人は英国のミルブルックで開催された Cenex Low Carbon Vehicle Event に Bosch 社と共に参加しました。INCA-TOUCH と ETAS ハードウェアを搭載した ETAS デモカーが、ここでも注目の的でした。

New Office in Japan

日本の新オフィス

顧客企業とパートナー企業から40名近くのお客様をお迎えして、日本の名古屋新オフィスの開所式及び懇親会をとり行いました。自動車産業の重要な役割を担う西日本地域にて、フィールドアプリケーションエンジニア5名とキーアカウントマネージャ2名の7名体制でETASのビジネスの成長を推進していきます。ETAS GmbHの代表取締役社長であるFriedhelm Pickhardは、開会の挨拶で「名古屋新オフィスにより、ETASは日本市場の需要や動向に対応していくことができます。ETASのソリューションとサービスは、組み込みシステムの開発と保守における品質と効率を高めてまいります」と述べています。今回の新オフィス開設は、ETASが日本で、そして自動車業界で成功し続けていくためには極めて重要なステップとなります。

執筆者

Anja Krahl
ETAS GmbH
 プレス・広報担当
 上級マネージャ



2017年2月17日に開催されたETAS名古屋新オフィスの開所式

ETASがTrustPointを買収

ETAS Acquires TrustPoint

ETASは、TrustPoint Innovation Technologies, Ltd.の買収により、サイバーセキュリティ機能を強化し、コネクテッドカー、スマートシティ、IoT（モノのインターネット）に対応する高度に制約された組み込みシステムの安全性とセキュリティソリューションを提供していきます。TrustPoint Innovation Technologies, Ltd.は、V2X（車車間・路車間通信）アプリケーション向けの組み込みセキュリティソリューションと、IoT用のセキュアなM2M（マシンツーマシン）通信を専門とする企業です。同社はこのたびの買収により、カナダのオンタリオ州ウォーターローに拠点を置くETASエンベディッド・システムズ・カナダ社に完全に統合され、同じくETASの子会社であるESCRYPT GmbHとの協働により組み込みシステム用セキュリティソリューションを提供してまいります。

契約書の調印を終えた Sherry Shannon-Vanstone（TrustPoint Innovation Technologies, Ltd.の社長兼CEO）と David MacFarlane（ETASエンベディッド・システムズ・カナダ社のマネージングディレクタ）





escar USA 2017

産学官が結集

ETAS と ESCRYP T は、今年で 5 回目となる、サイバーセキュリティのリスク、脅威、脆弱性について議論するサイバーセキュリティの国際シンポジウム、escar USA (Embedded Security in Cars) のホスト役を務めました。

今年のカンファレンスは 6 月 21 ~ 22 日の 2 日間、ミシガン州の大都市、デトロイトで開催されました。escar カンファレンスは、2003 年にドイツのケルンで開催された小規模の専門的なワークショップから始まりました。以来、ヨーロッパでは毎年開催され、2013 年からは米国で、そして 2014 年からはアジアでも開催されるようになりました。

escar USA は、討論の場を提供することによって、最新の車載サイバーセキュリティの脅威と適切な対策に関して産官学の協働を促すことを目指しています。この目標通り、今年のイベントでは 3 つの異なる分野で 300 名以上の多彩な参加者を動員して、自動車のサイバーセキュリティへの実践的アプローチについて議論しました。

19 名のプレゼンターは多彩な経歴の持ち主です。Paul Rosenzweig 氏

(Redbranch Law and Consulting) が「サイバーセキュリティの責任の進展状況」の説明で会場の雰囲気盛り立てました。他のプレゼンテーションでは、「自動車制御システムにおけるコンテキストウェアな侵入検知」、「車両環境と V2X アプリケーションにおけるエントロピーとランダム性」、「車両とモバイルの接続におけるリスクとセキュリティの評価」などのトピックが論じられました。

プレゼンテーションの質が一貫して高いのは、選定のプロセスがしっかりしているからです。プレゼンターの候補者はブラインドプロセスを通して自分のプレゼンテーションの書類をプログラム委員会に提出します。提出された書類は、少なくとも 3 名のレビュアーがそれぞれ個別にレビューします。今年のアクセプト率は 27% だったので、今回のプログラムに採用されたのは提出された書類のわずか 4 分の 1 程度だったことになります。人脈作りもこのイベントの重要な要素でした。参加者は、初日のプレゼンテーション後に執り行われるカクテルタイムや締めくくりのアウトドアディナーなど、人脈作りには十分な機会を得ることができ

ました。参加者は夜遅くまで野外に残り、炉辺の火でマッシュマロを焼きながら会話を楽しんでいました。

イベント後の参加者からのフィードバックでは、圧倒的にポジティブな意見が多く見られ、あるレビュアーは、escar を米国大統領の一般教書演説にたとえて「escar は自動車サイバーセキュリティの『一般教書演説』であると評判になっています。これからもずっと続けてください！」と言葉を寄せてくださいました。私たちはこの言葉を心に刻み escar USA 2018 を企画してまいります。

escar USA 2018 は 2018 年 6 月 20 ~ 21 日に開催されます。
詳しくは www.escar.info/escar-usa をご覧ください。

ETAS、ESCRYP T、そして最近 ETAS ファミリーに加わった TrustPoint Innovation Technologies, Ltd. の社員が一丸となり escar USA 2017 をホスト

執筆者

Claudia Hartwell
ETAS Inc.
(米国、ミシガン州
アナーバー)
マーケティング
コミュニケーション
上級専門家

10 Years ETAS Automotive India

ETAS Automotive India の 10 年

執筆者

Sameera C Damle
ETAS Automotive
India Pvt. Ltd.

(インド、バンガロール)
テクニカルセールス・
エンジニアリング
ソリューションズ部門長

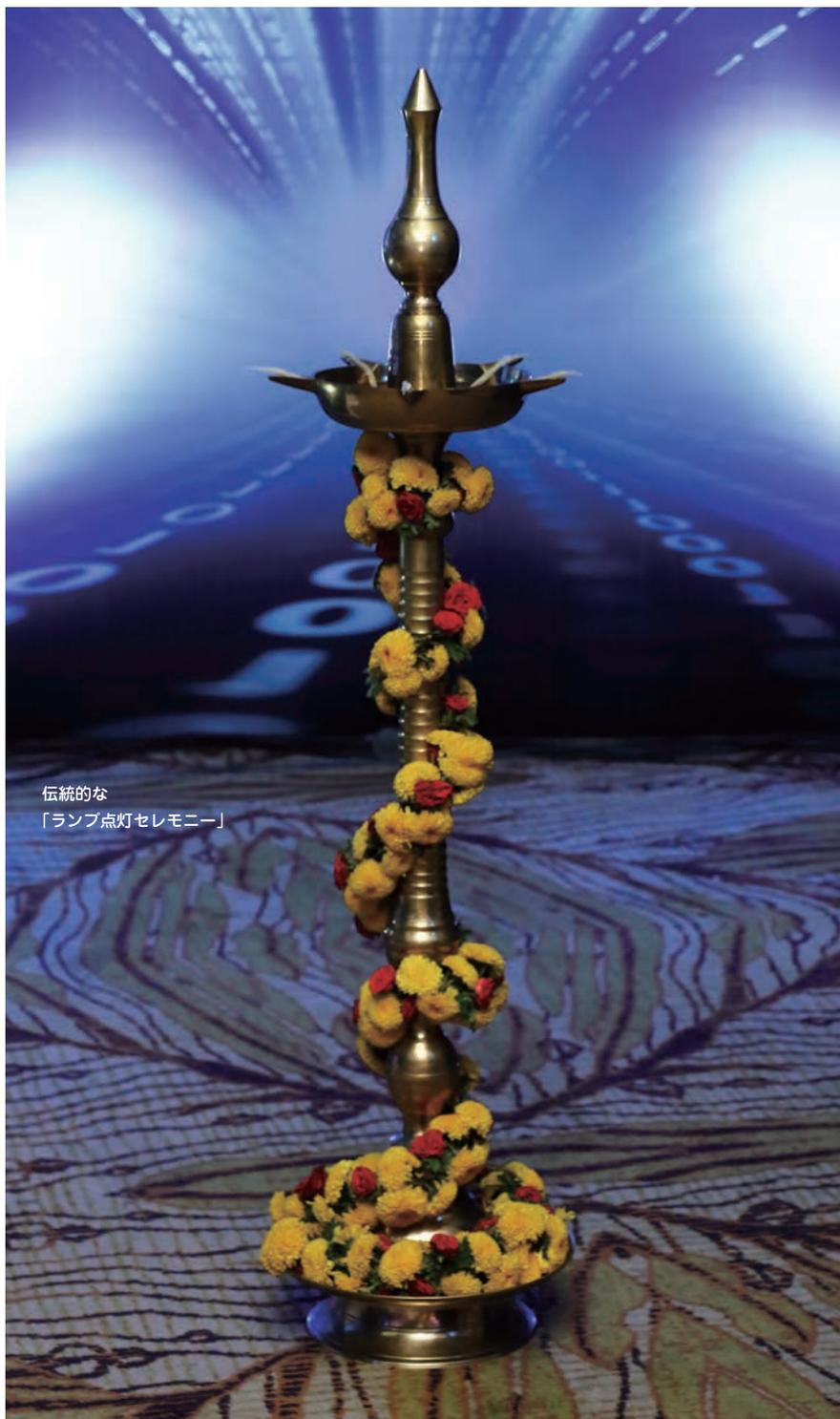
Rashmi Rao
ETAS Automotive
India Pvt. Ltd.

(インド、バンガロール)
エンジニアリング
テストソリューションズ
マネージャ

ETAS インド法人は、これまでの道のりで最も大切な存在である「お客様」をお迎えして、10周年の記念式典を挙行了しました。8月2日、50名のエグゼクティブを来賓者としてバンガロールにお招きし、ETASのこれまでを振り返り、今後の見通しを発表しました。ETASからは、経営陣を代表してFriedhelm Pickhard (ETAS GmbH 代表取締役社長)、Wolfgang Siemel (ETAS グループアジアパシフィック統括ヴァイスプレジデント)、Mahavir Patil (ETAS インド法人 統括マネージャ) が列席しました。

式典の幕開けとして、インドの伝統的な「ランプ点灯セレモニー」が執り行われました。それはまさに輝かしい未来に向かう歩みを象徴するものでした。続いて、伝統の継承と技術の発展を表す「デジタルランプ点灯」がLEDスクリーンに展開されました。この10年間のETASの歩みを紹介する簡単なビデオの上映に先立ち、お集まりの皆様にはMahavir Patilから歓迎のご挨拶をさせていただきました。Friedhelm Pickhardからは、自動車用ソフトウェア開発の未来についてETASが描いている構想をお話しさせていただきました。

お客様との質疑応答のセッションでは、2020年に導入されるバーラト・ステージ6(BS6)という排気ガス規制基準から、インドや他の国々における電動化、さらには組み込みセキュリティの領域に至るまで、幅広いテーマに関して、ETASの経営陣がさまざまな質問に答えました。今後直面する非常に重要な新興国のメガトレンドについて、ETASの考えを明確に伝えるために、「テクノロジーシ



伝統的な
「ランプ点灯セレモニー」

ETAS インド法人がお客様と一緒に 10 周年を祝いました

2017 年は ETAS インド法人にとって節目の年でした。同社は 2007 年に従業員 3 名で事業を開始しました。最初の仕事は、インドの 2 社のお客様に計測・適合ソリューションを提供することでした。現在は、従業員数が 40 名になり、ETAS のあらゆる製品とサービスを生かしたソリューションを提供しています。インドの OEM 企業（Mahindra、Tata Motors、Force Motors、Bajaj、Hero Honda など）や、世界トップの Tier 1 企業、OEM 企業のインド子会社またはインド事業部（Maruti Suzuki India Limited、Hyundai、Volkswagen、Renault、Nissan、Honda、Continental、Delphi、Denso、John Deere、EATON など）など、インド各地にある 150 社のお客様にご利用いただいています。



質疑応答セッションで回答する経営陣（左から右）：Wolfgang Siemel（ETAS グループ アジアパシフィック統括ヴァイスプレジデント）、Friedhelm Pickhard（ETAS GmbH 代表取締役社長）、Mahavir Patil（ETAS インド法人 統括マネージャ）

アター」が披露されました。その中で、ETAS インド法人の専門家が、「ADAS（先進運転支援システム）」「ビッグデータ」「仮想化」「電動化」「安全&セキュアなソフトウェア」の主要 5 項目における今後の ETAS のソリューションを紹介しました。お客様は将来に対する ETAS のビジョンについて強い関心を示し、またそれらのソリューションについて ETAS の技術専門家と詳細な論議を繰り広げました。

式典の締めくくりとなる晩餐会の前に、参加者の皆様に「ジェンベ」というアフリカの打楽器に触れていただく機会を用意しました。参加した方々は、打楽器奏者のチーム Taal Inc. による手ほどきを受けながら、それぞれが音楽に合わせてドラム演奏を楽しみました。こうして会場全体が笑顔に包まれて、晩餐会の雰囲気を楽しく盛り上げました。

わずか 10 年で、ETAS インド法人の若いチームは、インドでの優れた組み込み技術（エンベデッドエクセレンス）の推進に今後も長年にわたって期待されるまでに成長しました。

Close to the Customer

お客様の身近に

執筆者

Selina Epple
ETAS GmbH
編集者

Hans-Jürgen
Schmidt-Fürst
ETAS GmbH
グローバルカスタマー
サポートディレクタ

Norbert Seidler
ETAS GmbH
サポートエンジニアリング
専門家

ETAS のカスタマーサポート

ETAS では、製品の納入前後に優れたサポートを提供することに注力しています。ETAS サポートチームはお客様とのパーソナルなつながりを特に重視しています。なぜなら、個々のお客様の懸念事項に対してよりきめ細かく対応することができるからです。

よくあるサポート体験：あなたは今、ツールの操作方法に困っていますが、サービスプロバイダの電話番号も E メールアドレスもわかりません。仕方なく、一般的なお問い合わせ用の入力フォームに問題点を入力します。そして数日間待たされた後、ありきたりの回答を受けることとなります。

チャットボット、アバター、人工知能を使用してサポートを匿名化する傾向にある中で、ETAS はパーソナルなサポートに重点を置き続けています。ETAS が毎年実施しているお客様満足度調査では、お客様自身がパーソナルなつながりの重要性を理解し高く評価していることが明確に示されています。ETAS は、他のサポートチャンネルの提供にも取り組んでいますが、最優先事項はお客様の身近な存在であり続けることに変わりはありません。

迅速で簡単 — チームの力による適切なサポート

ETAS はすべての ETAS オフィスで、電話と E メールによる高品質のサポートをお客様に提供しています。多数の豊富な経験を積んだ、高い技術を誇るスタッフが対応しているため、ほとんどのサポートリクエストは直ちに処理されます。

ETAS では、弊社サポートフォリオの特定の分野を専門とするスタッフがチームとなって、効果的にサポートを提供しています。これらのサポートチームが一丸となって取り組むことにより、ETAS では、

以下のようなさまざまなレベルのサポートを提供することができます。

- 第 1 レベルのサポート：迅速かつ直接的な問題の報告と解決策の提供
 - 第 2 レベルのサポート：具体的な質問に特化した次のレベルのサポート。第 1 レベルのお電話によるサポートでは解決できないお問い合わせの処理
 - 第 3 レベルのサポート：特に専門的なお問い合わせや複雑な要件への対応
- 専門知識は Wiki データベースに内部文書として蓄積されています。昨年から FAQ 形式で社外にも提供されるようになりました。ご好評いただいている FAQ は、ETAS ウェブサイトのダウンロードセンターからアクセスすることができます。

お客様の近くに

ETAS はサポートホットラインに加えて、オンサイトサポートも提供しています。ETAS の常駐エンジニアは、ユーザーにとって重要な窓口となります。常駐エンジニアは、製品の使用のサポートはもちろんのこと、お客様のプロセスやツールに製品をすばやく効率的に統合させるお手伝いもしています。

お客様にオンサイトサポートを提供するのは常駐エンジニアだけではありません。ETAS ホットラインの専門家がお客様を訪問することもあります。これにより、お客様との関係が強化されるだけで

なく、お客様のワークプロセスに関する ETAS 社内の知識も向上します。また、サポートの質も継続的に高めていくことができます。さらに、ホットラインスタッフの日常業務にもメリハリややりがい生まれ、それがまた彼らの強みとなります。これは仕事の質と同様に重要なことです。

路上でのサポート

近年、ETAS サポートエンジニアはスウェーデンや南アフリカなどで実施される多くのテスト走行プロジェクトに同行しています。特に注目すべき一例は、スペインのグラナダ県で実施されるテストでの 3～4 週間にわたるサポートです。これは、数年前から ETAS が自主的に取り組んでいるものです。シエラネバダの山々は、高低差が 2,600 メートルにも達するため、温度変化が非常に厳しく、自動車メーカーが自社の車の力量を試すのには理想的な環境です。この場所で多くの自動車メーカーやサプライヤーが進んで ETAS にサポートを依頼していただくことは、当然のことといえるでしょう。

お客様からのきわめて好意的なフィードバックが原動力となり、ETAS サポートチームは、多くの技術的課題にもかかわらず、人とのつながりを最優先に成果をあげ続けています。



理論で現実に対応 — 使用事例

お客様に貢献する ETAS サービスパッケージには、ETAS ウェブサイトのダウンロードセンターで入手できる使用事例もあります。ユーザーがユーザー向けに書いた使用事例では、運用シナリオや、さまざまなヒントやコツを紹介しています。たとえば、ツールの使用方法と面倒な問題をユーザー自身がツールで解決する方法を紹介しています。これにより、ユーザーはツールを、一般的に想定されるシナリオの域を超えて最大限に活

用できるようになります。使用事例の多くは、お客様のプロジェクトやワークショップ、あるいは具体的なお問い合わせから得られた経験に基づいています。そのため、日常的なシナリオから直接、関連する問題を考察することができません。ETAS は自社のハードウェアとデータを用いて使用事例を再現しているので、元々のお客様が特定されることは決してありません。

ETAS サポートチームは、場所や内容を問わず、いつでもお客様をお手伝いします！

ETAS and Lynx Software Technologies Collaborate

ETAS と Lynx Software Technologies 社が協業

ETAS と Lynx Software Technologies 社は、次世代のコネクテッドカーや自律走行車のニーズに対応できる、安全でセキュアな ECU プラットフォームの技術を共同で提供していきます。これにより、セーフティクリティカルなアプリケーションの開発に最高水準のサイバーセキュリティが加わり、自動車業界に新たな可能性をもたらします。次世代のコネクテッドカーや自律走行車の場合、「EE アーキテクチャ」として高性能のドメインコントローラ (DC-ECU) や車載コンピュータ (VC-ECU) を導入する必要があります

が、適応性に優れ充実したソフトウェアプラットフォームを備える高性能のマイクロプロセッサを採用したこれらの ECU は、安全性、セキュリティ、リアルタイム性における難題を抱えているうえ、一般的なプラットフォームとの統合も可能でなければなりません。ETAS と Lynx Software Technologies 社が提供するソリューションは、このような DC/VC ECU に必要とされる安全でセキュアな信頼性の高いソフトウェア基盤を実現します。

STMicroelectronics 社、 ETAS、ESCRYPT: コネクテッドカーのための セキュアアプリケーション

STMicroelectronics, ETAS, and ESCRYPT: Secure Applications for Connected Cars

ETAS と ESCRYPT は、電子制御アプリケーション用半導体の世界的メーカーである STMicroelectronics 社 (New York Stock Exchange: STM) との協業で、コネクテッドカー時代に即した新しい車両制御装置の開発を高速化する、マイクロコントローラ、ソフトウェアツール、およびセキュリティソリューションで構成される完全なプラットフォームの提供を目指しています。このプラットフォームにより、各種ネットワークを介した車両へのアクセスを可能にしながら、車両所有者のプライバシーや OEM の知的財産権、ECU 機能などの高度な保護を実現するセキュア ECU を構築することができます。

この共同ソリューションでは、電力効率が高くリアルタイム制御に対応できる STMicroelectronics 社の SPC58 シリーズの車載用マイクロコントローラを採用しています。このマイクロコントローラはハードウェアセキュリティモジュール (HSM) を内蔵し、最新式の通信インターフェース (CAN FD、LIN、FlexRay、タイムスタンプ機能付き Ethernet など) を搭載しています。またセキュアエレメントやエンベデッド SIM (Subscriber Identity Modules) などより、ECU やゲートウェイに対するインターネット経由の攻撃からも防御できます。一方、ESCRYPT は OTA (Over-The-Air: 無線) ソフトウェアアップデートなどのセキュア ECU 用通信技術を結集し、SPC58 HSM 用のファームウェアやミドルウェアも提供しています。HSM と ESCRYPT のセキュリティ技術とが一体となって、信頼できるソースを認証し、不正アクセスを阻止します。オペレーションシステムには、ECU コード用リアルタイム OS として定評のある ETAS の RTA ソフトウェアを採用しており、さらに RTA-BSW (基本ソフトウェア) を補完する ISOLAR-A ツールや ISOLAR-EVE ツールを使用することにより、仮想環境で ECU ソフトウェアスタック全体の構築とテストを行うこともできます。

ESCRYPT が Renesas Electronics 社と 協業

ESCRYPT Collaborates with Renesas Electronics

先進の半導体ソリューションにおいて世界をリードする Renesas Electronics Corporation が ETAS の子会社 ESCRYPT と共同で、自動運転用の複雑な車載アプリケーションにセキュリティ機能を統合するための新しいプラットフォームソリューションを開発しています。ここでハードウェアプラットフォームとして採用しているのは、機能安全、セキュリティ、車両制御ネットワークなどの技術をワンチップに結集した Renesas 社の車載用セーフティマイクロコントローラ RH850/P1x-C シリーズで、ソフトウェアプラットフォームとしては ESCRYPT のハードウェアセキュリティモジュール用セキュリティソフトウェアスタックの CycurHSM を採用しています。この新しいプラットフォームソリューションにより、非常に複雑な車載セキュリティ機能の実装と開発時間の短縮が実現できるので、安全機能とセキュリティ機能の統合が加速され、全自動運転の実現への足がかりとなることでしょう。

執筆者

Anja Krahl
ETAS GmbH
プレス・広報担当
上級マネージャ

ETAS Locations Worldwide

Germany

Stuttgart
(Headquarters)

Brazil

São Bernardo do Campo

Italy

Turin

Sweden

Gothenburg

Canada

Waterloo, Ontario

Japan

Nagoya
Utsunomiya
Yokohama

United Kingdom

Derby
York

France

Saint-Ouen

Korea

Seongnam-Si

USA

Ann Arbor, Michigan

India

Bengaluru
Chennai
Gurgaon
Pune

P.R. China

Beijing
Changchun
Chongqing
Guangzhou
Shanghai
Wuhan

ETAS GmbH, Borsigstraße 14, 70469 Stuttgart, Germany · Executive Board of Management: Friedhelm Pickhard, Bernd Hergert, Christopher White · Chairman of the Supervisory Board: Dr. Walter Schirm · Registered office: Stuttgart · Court of registry: Lower District Court (Amtsgericht) of Stuttgart, HRB 19033

Managing Editor: Tatiana Bohlmann · **Editorial Team:** Nicole Bruns, Jürgen Crepin, Claudia Hartwell, Anja Krahl, Silke Kronimus, Dr. Ulrich Lauff, Andrea Müller · **Authors contributing to this issue:** 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 · **The following articles have already been published as a long version in:** Elektronik automotive, (p. 5-7, p. 8-11); Hanser automotive (p. 14, p. 30-31), ATZelextronik (p. 12-13, p. 32-34), Automobil Elektronik (p. 26-27), ATZextra (p. 28-29) · **Production management and design:** vogt grafik · **Translations:** Burton, Van Iersel & Whitney GmbH · **Printing:** Gmähle-Scheel Print-Medien GmbH · **Circulation:** German, English, Japanese: 13,800 **Figures:** DKG Photography, ESCRYPT, ETAS, fotolia, FSG Schulz, Hochschule Kempten, Hyundai R&D Center, iStockphoto, René Müller Photographie, Robert Bosch GmbH, shutterstock

© Copyright: 12/2017 ETAS GmbH, Stuttgart – All rights reserved. The names and designations used in this publication are trademarks or brands belonging to their respective owners. RealTimes is printed on chlorine-free, bleached paper. Printing inks and varnishes are environmentally safe, made from renewable resources, and contain no mineral oils. www.etas.com

日本語翻訳・印刷協力：株式会社翻通・Dooree Design Co.,



RealTimesをお読みいただき、ありがとうございます。
ETASの**RealTimesオンライン**ニュースレターでは、
本書の補足情報および世界中のETASから寄せられる
最新の話題を定期的に配信しています。

- ETAS製品の活用事例およびサクセスストーリー
- 技術記事
- 会社情報
- トレーニングおよびイベント情報
- インタビュー
- FAQ

登録フォームおよび過去の**RealTimesオンライン**は、
下記リンクよりアクセスしていただけます。

www.etas.com/Rto



RealTimes online

NEWS

Anniversary in India, Support in Spain, Formula Student in Germany

Dear Sir or Madam,

we are happy to present you our fall issue of RealTimes online with a mix of different topics, including a technical article about cyber security, news from ETAS Customer Support and retrospects of the 10 years anniversary celebration of ETAS India and the Formula Student Germany 2017.

Enjoy reading!

Best regards,
Your ETAS team

Are you secure?
Automotive electronics are undergoing radical change. We face major challenges with new powertrain concepts, (partially) automated driving, and connection to the Internet of Things (IoT). We are already capable of implementing high-quality electronic systems in large numbers with the highest safety requirements, and this will continue to be important. However, it will no longer suffice on its own, because connected vehicle systems require additional protection against unauthorized access to their data and functions. It also means our software development will no longer end with the start of production (SOP).

[read more](#)

Customer satisfaction grows continuously
The ETAS Support Team uses its annual survey to monitor customer satisfaction on a regular basis. This not only helps identify the drivers of satisfaction, but it also uncovers potential for improvement. The findings are particularly important for achieving a major goal: a continuous improvement in customer satisfaction. The latest survey results show that ETAS Support was able to meet its goal – and is already working to optimize the quality of its services even further.

[read more](#)

New version of ETAS MDA is available
The latest version 8.2.0 of the ETAS MDA (Measure Data Analyzer) was released at the end of September and is available in the Download Center. In addition to a number of improvements, especially in terms of usability, the main innovations are: the combined usage of the MDA and the EHANDBOOK-NAVIGATOR, a new instrument to quickly obtain a list of occurrences of Boolean edges and the possibility to visualize bounds in the scatter plot. An overview and description of all new features can be found by clicking on the "What's new?" button.

[What's new?](#)

10 years ETAS Automotive India
ETAS India celebrates its 10th anniversary together with its customers. Fifty executives from senior management were invited to Bangalore to relive the journey ETAS has taken and to take a look at the journey ahead.

[read more](#)

ETAS and its logo are the scatter plot. All other content is copyright of ETAS. All rights reserved. 2017