ルネサスと ESCRYPT が車載 ECU に高いレベルのセキュリティを提供するハードウェア／ソフトウェア統合ソリューション開発で協業

～自動運転時代の複雑な車載アプリケーションへのセキュリティ実装を容易にする新しいハードウェア／ソフトウェアの統合ソリューション～

2016 年 11 月 09 日
ルネサス エレクトロニクス株式会社
ESCRYPT GmbH

ルネサス エレクトロニクス株式会社（本社：東京都江東区、代表取締役社長兼 CEO:呉文精、以下ルネサス）と組み込み向けセキュリティソリューションを手がける ESCRYPT GmbH（本社：ドイツ、マネージングディレクタ：Dr. Thomas Wollinger、以下 ESCRYPT）はこのたび、自動車用の電子制御ユニット （Electronic Control Unit: ECU）に必要とされる高いレベルのセキュリティを提供するハードウェアとソフトウェアの統合ソリューション開発で協業することを発表いたしました。

この新しいハードウェア／ソフトウェアの統合ソリューションは、ワンチップ上に機能安全技術と車載制御ネットワーク技術を搭載したルネサスの車載用マイコン「RH850/P1x-C シリーズ」と ESCRYPT のセキュリティソフトウェア「CycurHSM」を組み合わせたもので、高度な車載セキュリティソリューションを実現します。 新ソリューションは自動運転に対応した複雑な車載 ECU アプリケーション向けセキュリティの開発や実装にかかる期間を短縮し、世界中のクルマにいち早く安心と安全を提供します。

自動運転などの高度運転支援システム（Advanced Driver Assistance Systems: ADAS）に対応したクルマでは、車両内インフォテイメント、車車間通信（V2V）、路車間通信（V2I）といったネットワークへの接続が見込まれ、これらのネットワークから、運転をサポートするための道路状況やその他の情報を獲得できるようになります。このことは、外部からの不正なアクセスに対してシステムが守られていることを保証する、強固なセキュリティが求められていることを意味しています。

ルネサスの車載用マイコン、RH850/P1x-C シリーズは、車両システムに求められる非常に厳しいセキュリティ要件に対応するために、データの暗号化や認証、乱数生成をサポートするコプロセッサを搭載したハードウェア・セキュリティ・モジュール（Hardware Security Module: HSM）を内蔵しています。また RH850/P1x-C シリーズ向けに最適化された CycurHSM は、セキュアブートなどのセキュリティサービスを提供することによってハードウェアのセキュリティを補強します。

このたび両社が開発したハードウェア／ソフトウェア統合ソリューションは世界中で利用可能であり、車外のネットワークと接続される自動運転のクルマに高い付加価値を提供し、セキュリティの問題を解決することができます。

このハードウェア／ソフトウェア統合ソリューションの特長は以下のとおりです。

（1）自動運転時代のクルマに求められる安心と安全をいち早く届けるための統合ソリューション

ハードウェア／ソフトウェアの統合ソリューションは、ECU に最高レベルのセキュリティを保証する ESCRYPT のソフトウェアである CycurHSM と、安全な制御を実現する ICU-M（注 1）を搭載したルネサスの 40nm（ナノメートル、ナノは 10 億分の 1）プロセス車載用マイコン、RH850/P1x-C シリーズで構成されます。

ICU-M は、秘密鍵および公開鍵暗号方式に基づいたセキュリティ機能を提供し、現在想定されている高度なサイバーセキュリティ攻撃への対応が可能です。また、専用のコード／データフラッシュ、複雑な暗号モードを備える高速 AES コプロセッサ（注 2）、AIS-31（注 3）に準拠した真正乱数を主とする疑似乱数生成など多くのセキュリティ機能を有しています。

CycurHSM は、SHE/SHE+（Secure Hardware Extension）規格の要求する機能に加えて、セキュアなフラッシュ書き込み、セキュアな ECU 間通信、その他様々なセキュリティ機能を実現するスケーラブルなソリューションであり、HSM を活用したセキュリティ機能を最大限に引き出す専用のインタフェースを有しています。これらの技術の融合によって生まれたこの統合ソリューションは将来のクルマに求められる安心と安全をすぐに提供することができます。

（2）セキュリティに関するソフトウェア開発期間を最大 90%短縮

RH850/P1x-C シリーズ を使用した ECU 開発では、ルネサスと ESCRYPT から提供されるセキュリティの実装を容易にする最適なソリューションを使うことができます。今回発表するハードウェア／ソフトウェアの統合ソリューションは AUTOSAR に完全準拠となっているため、

既存の AUTOSAR アプリケーションに対するセキュリティソフトウェアの開発は簡単な設定のみで済ませることができるため、その開発期間を最大 90%削減可能です。一方、新しいアプリケーションについても AUTOSAR への準拠・非準拠に関わらず、ソフトウェアの下位レイヤまたはハードウェアに依存する設計の考慮が不要なため、上位レイヤのソフトウェア開発に集中できます。このため、車載 ECU の開発全体にかかる期間を少なくとも 50%削減可能となります。

(3) 自動運転車への付加価値としてさらに最適化されたセキュリティサービスを利用可能

今回開発するソリューションは、リスク分析や効果的なセキュリティコンセプトの構築だけではなく、鍵管理といった追加のセキュリティサービスを活用することでさらに機能を拡げることが可能で、ESCRYPT の親会社である ETAS などにより提供される AUTOSAR スタックへ統合することができます。

ルネサスと ESCRYPT の協業によるハードウェア／ソフトウェアの統合ソリューションによって、クルマの遠隔ハッキングなどの新しい問題を防ぐ堅牢なセキュリティへの対応をはじめ、ハードウェア、ソフトウェアの幅広い分野をカバーする、品質の高いターンキー・ソリューションが提供されます。

世界中で利用可能なこのソリューションは、ネットワークに接続される自動運転をはじめ ADAS に対応したクルマのセキュリティを高め、セキュリティ問題を解決することができます。

ESCRYPT について

ESCRYPT – Embedded Security は世界をリードする組み込みセキュリティシステムのプロバイダです。ドイツ、英国、スウェーデン、米国、カナダ、中国、韓国、および日本に拠点を構え、セキュア M2M（Machine to Machine）通信、「モノのインターネット（Internet of Things、IoT）」における IT セキュリティ、e-ビジネスモデルの保護や自動車のセキュリティなどといった最新のセキュリティトピックに関してお手伝いできるセキュリティのスペシャリ ストをそろえ、世界中で高く評価される非常にセキュアな製品やソリューションを開発しています。それらの製品やソリューションは、組み込みシステムおよび 関連する IT インフラストラクチャの固有の要件に合わせて作られ、何度もテストされて、自動車の生産で効果が実証されています。

ESCRYPT 社は、Bosch Group の子会社である ETAS GmbH のグループ会社です。詳細につきましては www.escrypt.com をご覧ください。

ETAS について

ETAS は、自動車産業をはじめとするさまざまな領域における組込みシステム開発向けに、革新的なソリューションを提供しています。システム・プロ バイダの ETAS のポートフォリオは、統合ツールおよびツール・ソリューションからエンジニアリング・サービス、コンサルティング、トレーニング、および サポートまでを多面的に網羅しています。組込みシステム領域のセキュリティソリューションは、ETAS の子会社である ESCRYPT 社によって提供されます。1994 年に設立された ETAS GmbH は、Bosch グループの 100%子会社として、欧州、北・南米、アジア地域で子会社、セールス・オフィスを展開しています。詳細につきましては www.etas.com をご覧ください。

- （注 1）

  データの暗号処理や乱数発生に対応するコプロセッサを搭載したルネサス製のハードウェア・セキュリティ・モジュール

- （注 2）

  AES は Advanced Encryption Standard の略で、国商務省標準技術局(NIST)によって制定された、米国標準暗号化方式

- （注 3）

  非決定論的乱数生成器について定めた規格

- ＊ 本リリース中の製品名やサービス名は全てそれぞれの所有者に属する商標または登録商標です。

ニュースリリースに掲載されている情報（製品価格、仕様等を含む）は、発表日現在の情報です。その後予告なしに変更されることがございますので、あらかじめご承知ください。