ホワイトペーパー

IoT 化に向けた通信モジュールのニーズについて

Naoyuki Tsubaki, IoT Product Marketing Department, Renesas Electronics Corp.

2019 年 7 月

概要

IoT 化の急速な普及に伴い、従来ネットワークに接続していなかった様々な機器においても今後益々、通信モジュール機能の搭載が加速されてきている。一方で、セキュリティの脅威も増大化してきている。その為、マイクロコントローラには、省フットプリント、低消費電力、セキュリティ、OTA によるタイムリーな Firmware アップデート機能の実現等が求められる。

はじめに

インターネット技術および各種センサ技術が飛躍的に向上してきたことにより、あらゆる分野や用途で機器の IoT 化が加速。市場予測会社のデータによると IoT デバイスの市場規模は 2022 年までに 1 兆米ドル規模にまで成長すると予測されている。IoT 機器の用途や目的に応じて様々な規格の通信モジュールや各種センサモジュールを搭載するエッジデバイスでは、モジュールの小型多機能化が進み、そこに搭載するマイクロコントローラにおいても従来の高性能・低消費電力に加えて、小型パッケージの要求が市場ニーズとして増えつつある。

また、アプリケーション開発の側面においても、IoT 化に伴う付加価値機能の追加、各種通信 I/F のプロトコルスタックに対応したプログラムコード開発なども伴うため、制御が複雑になり、コードサイズも増えつつあることから、マイクロコントローラには高性能 CPU に加えて、大容量 Flash ROM /RAM の搭載が求められるようになってきている。加えてハードウェア設計者目線では、製品ラインアップが多様化し、出来る限り基板開発を共通化した最適化設計（プラットフォーム設計）による開発費削減も求められており、ピン配置や外形の互換性のある小型パッケージでかつ、ハイスペックなマイクロコントローラが理想的と考えられている。

更に、インターネット接続を伴う IoT 機器では、それ自身つまり、IoT 機器のエンドポイントにおけるセキュリティの重要性も認識が広がってきている。近年では、ネットワークに接続した IoT 機器を踏み台にしたサイバー攻撃や、機器の乗っ取りや覗き見といったセキュリティの脆弱性を突いたインシデントも増えてきており、セキュリティ対策への関心が益々高まってきている。セキュリティ対策が不十分なままの機器は、常にハッカーによるハッキングや乗っ取りなどの脅威に晒されてしまう為、こういった問題を解消するためにもエンドポイントであるエッジデバイスへのセキュリティ対策の導入は必要不可欠となってくる。例えば、製造/出荷工程の安全なプログラム書込み出荷や、市場投入後に万が一、プログラムコードに不具合があった場合のセキュリティパッチ対応が必要となるなど、製品の

ライフサイクル全体のマネジメントも重要になってくる。これらの対策には、従来のコントローラに加えてセキュリティ専用 IC の搭載や、セキュリティ知識に長けた有識者を備えた開発が迫られるが、常にコスト削減や開発 TAT 短縮化を求められるエッジデバイスにおいては導入障壁が高いケースが多く、マイクロコントローラ内にこれらの機能が搭載されていることが望ましい。

このホワイトペーパーでは、これら IoT エッジデバイスに搭載される機器に求められる要件を解説する。

省フットプリントと高性能の両立

小型モジュールの開発には、制御をつかさどる中心のマイクロコントローラ自身にも小型パッケージが要求される。例えば市場にある通信モジュールの基板サイズはおよそ 10mm x 10mm がラインアップされているため、5mm x 5mm 以下となるような小型パッケージが望ましい。更に、小型化が求められるだけでなく、多彩なアプリケーションに対応するための大容量 ROM や、プロトコルスタックのハンドリングのための大容量 RAM の搭載も同時に求められる。また、アプリケーション規模に合わせて適切なメモリ容量を選択可能なラインアップ展開が求められている。通常、マイクロコントローラにおいては、大容量メモリ搭載と、小型パッケージはトレードオフの関係にあり、一般的に両立が難しいと言われている。そのため、市場にある現状の小型パッケージ製品のラインアップは、1MB ROM/256KB RAM 製品が主流となっている。

今回、業界最先端の 40nm プロセス技術を採用した RX651 の新たなパッケージとして、最大で 2MB 内蔵 Flash ROM、640KB 内蔵 RAM を持ちながら、4.5mm x 4.5mm という小型パッケージの両立を実現した。　これによって、従来 RX651 ラインアップで最小サイズだった 7.0mm x 7.0mm パッケージに比べて、およそ 60%のフットプリント削減が可能となり、市場ニーズにも柔軟に対応することが可能となる。内蔵メモリとしては、Flash ROM は 512KB～2MB まで、RAM は 256KB or 640KB のメモリ容量展開となり、64 ピン小型パッケージ製品群として、メモリ容量を変更しても全てピン互換のパッケージを維持出来ることから、お客様の部品や基板設計を共通化したプラットフォーム設計、ラインアップ製品開発を容易に行うことが可能となる。

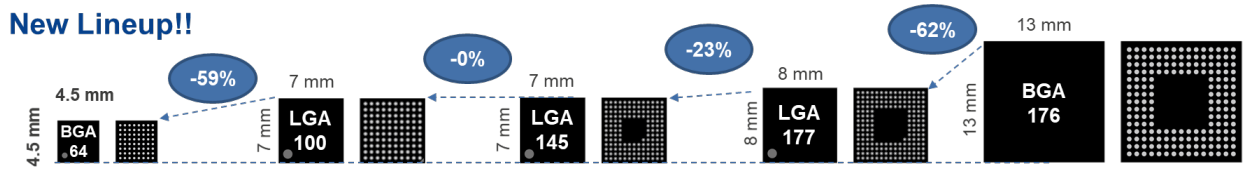

Figure 1: Small Footprint Package of RX651 64pin BGA

組込システムにおけるルートオブトラスト

一般的に組込みシステム開発において、セキュリティ機能実装に伴うハードウェアおよびソフトウェア開発には、セキュリティに長けた開発リソースの工面に加え、コストの観点からもハードルが高い。しかしその一方で、エンドユーザに対して価値を訴求するのが難しい側面を持っている。セキュリティ機能が非常に重要になる金融や秘匿情報を扱うアプリケーションにおいては、強固なセキュリティは付加価値として市場から認められるため、開発工数およびコストをかけて積極的に導入するケースも多く、このような市場では、セキュリティ専用 IC を用いて強固なセキュリティを実現してきた。

昨今、IoT 化に伴い、従来ネットワークにつながらなかった機器に関しても、セキュリティ導入を視野に入れるメーカが増えてきている。しかし、セキュリティに関する経験が不足し、かつ、汎用マイクロコントローラーを使い慣れている機器開発メーカーにとって、強固なセキュリティが汎用マイクロコントローラーで実現できることが合理的であり、エッジデバイス開発に求められているニーズとなっている。

また、ネットワークに接続する IoT 機器においては、クラウドやサーバー、またデータ送受信の中継地点となるゲートウェイやアクセスポイントで、安全が担保されない可能性もあることから、エンドポイントとなる IoT 機器自身で安全を担保する必要がある。これを実現するためには、Root of Trust(信頼の起点)をエンドポイント自身が持つ必要があり、この Root of Trust によって、機器に自律したセキュリティ(安心)を提供する事が可能になる。

Root of Trust を実現するための提案として、RX651 マイクロコントローラでは、「鍵データ」を漏えいから守る Trusted Secure IP や、「認証プログラム」を改ざんから守るメモリ保護機能がハードウェアとして備わっている。

RX651 の内蔵 Flash 1.5MB, 2MB 製品では、暗号鍵を管理する専用ハードウェア IP である Trusted Secure IP を内蔵することで、暗号鍵への不正なアクセスを遮断すると共に、暗号鍵を秘匿化(インデックス化)することで安全に内蔵 ROM 内に保管する機能を備えている。
加えて、RX651 全製品に搭載しているメモリ保護機能では、例えば内蔵フラッシュメモリの“エリアプロテクション機能“を使うことで、決められた領域に格納されたコードを外部から書き換え不可能な状態を作ることが出来る。これにより、不正コードを検出するコードそのものを守れるため、安全性を担保することが可能となる。

このように、RX651 製品群ではセキュリティ専用チップを使うことなく、汎用マイクロコントローラの搭載機能で強固なセキュリティを導入可能となる。

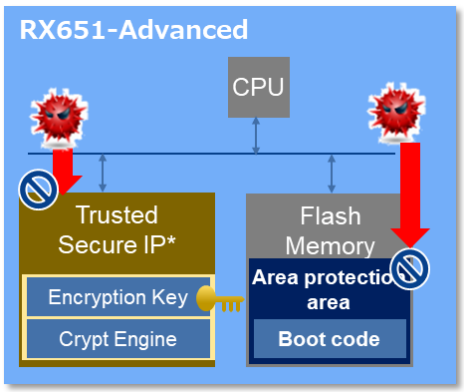

Figure 2: *Root of Trust by Trusted Secure IP and Area protection*

RX651 の Trusted Secure IP では共通鍵暗号方式である AES, 3DES などの対応に加え、SSL/TLS 通信に必要とされる公開鍵暗号方式 RSA などに対応しているため、各種クラウドサービスへの接続などに求められる暗号通信を HW ベースで行うことが可能となり、CPU 負荷をかけずに高スループットの通信を実現することが出来る。

容易なファームウェアアップデート

市場投入後の製品に対して、ネットワーク経由で新しい機能を追加、バグフィックス、強固なセキュリティを担保し続けるなど、IoT デバイスにおいてファームウェアのアップデート機能は必須の機能と言える。特にサイバー攻撃の手法の進化は著しく、市場投入後にパッチを当てる必要が出てくることも考えられる。従来、マイクロコントローラにおける FW アップデートは、専用に用意したバックアップ用のメモリに新しい FW をダウンロードし、アップデート専用のプログラムを実行することで実現してきた。しかしこの方法では、バックアップ用メモリを別途搭載する必要があることに加え、アップデート中はシステムを停止しなければならないなどの問題があった。そのため、このバックアップ領域を内蔵メモリとして搭載し、更にバックグラウンドでのダウンロードに対応出来ることが好ましい。

RX651 に搭載されている 2MB 及び 1.5MB のフラッシュメモリは、Dual bank 機能や Back Ground Operation(BGO)機能をサポートしており、システムを停止させることなく内蔵フラッシュメモリ単体で FW のアップデートを実現することが可能となっている。この Dual Bank 機能では、内蔵フラッシュメモリを 2 面の領域に区切り、実行領域と新しいファームウェアをダウンロードするテンポラリ領域に区切ることが出来る。BGO 機能を使うことで、実行領域のコードを実行しながら、通信インタフェースから新しいファームウェアを受け取り、テンポラリ領域に書き込んでいくことが可能となる。バックグラウンドでの書き込みが完了したところで、実行領域を切り替えるレジスタをセットし、リセットを発行することで新しいファームウェアの実行がはじまる。このとき、ファームウェアの破損をチェックするブートを導入しておけば、バックアップしている古いファームウェアに戻すことも容易に可能となる。

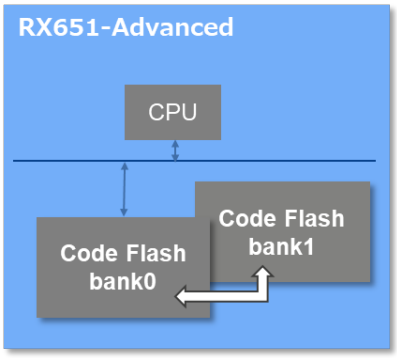

Figure 3:　Dual bank flash function

結論

IoT 向けモジュールに求められる、小型・大容量メモリ・セキュリティ・FW アップデート機能、これら全てを 1 チップで実現しつつ、アプリケーション規模に応じて最大 2MB ROM/640KB RAM まで選択可能な RX651 の 64pin パッケージは、コストアップすることなく IoT 機器を構築するための最適なマイクロコントローラと言える。