White Paper

Communication Module Requirements for IoT Applications

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

July 2019

Abstract

With the rapid spread of the IoT, many devices that were not connected to a network in the past increasingly require the integration of a communication module function. Conversely, the number and severity of security threats are also on the rise. Microcontrollers therefore must meet a range of demands, including smaller footprints, lower power consumption, enhanced security, and timely over-the-air (OTA) firmware update capability.

Introduction

Dramatic advances in Internet technology and various types of sensor technology are driving the trend toward IoT enablement of numerous devices used for a wide range of purposes. According to data published by market forecasting companies, the market scale for IoT devices is expected to grow to one trillion US dollars by the year 2022. Edge devices that incorporate communication modules for various standards along with specific sensor modules according to the application and purpose of the IoT devices are shrinking in size while also realizing multifunction capabilities. Consequently, the microcontrollers in such devices must meet market demands that include not only existing requirements such as high performance and low power consumption, but also more compact package dimensions and smaller footprints.

Furthermore, application development also involves the addition of value-added functions for IoT support and the development of program code to handle the protocol stacks for various communication interfaces. This increases control complexity as well as code size, which means that the microcontroller requires not only a powerful CPU but also ample flash ROM and RAM capacity. From hardware designer's point of view, the product lineup has become more diversified, and platform specific optimized design with board development being shared as much as possible is necessary in order to reduce development costs. The ideal is a high-spec microcontroller in a compact package that offers compatibility in terms of pin layout and shape design.

Since IoT devices by definition feature Internet connectivity, there is increasing awareness of the need for security at the IoT device itself, i.e. the endpoint. In recent years, there has been an increase in cyber attacks using Internet-connected IoT devices as a gateway, as well as incidents taking advantage of security vulnerabilities for hijacking devices or using them for snooping. This has made the implementation of suitable security measures an important

concern. If adequate measures are not in place, devices are constantly exposed to risks such as hacking and hijacking. In order to solve such problems, it is essential to introduce security measures on edge devices which serve as endpoints. This also points to the importance of overall life cycle management, which includes ensuring safe program writing during the original manufacturing and shipping process, as well as dealing with cases where a program code problem requiring a security patch is detected after introduction to the marketplace. The normal approach is to add a dedicated security device to a conventional controller and to pursue development in consultation with knowledgeable experts in security, but cost restrictions and the need to shorten turn-around time (TAT) often makes this difficult for edge devices. It is therefore desirable to integrate security functions in the microcontroller itself.

This White Paper describes the requirements for products to be installed in IoT edge devices.

Small Footprint and High Performance

The development of compact modules requires that the central microcontroller responsible for function control comes in a package with a small footprint. For example, the lineup of communication modules on the market commonly has a footprint of 10 x 10 millimeters, but smaller packages with 5 x 5 mm or less are desirable. Not only should the package footprint be smaller, but larger ROM capacity to support various applications as well as plenty of RAM for protocol stack handling are also needed. The lineup should offer the ability to select a suitable memory capacity according to the application scale. In a conventional microcontroller, memory capacity and small package footprint are in a tradeoff relationship and it is considered difficult to achieve both. As a result, the current lineup of small footprint controllers on the market is centered on 1 MB ROM/256 KB RAM products.

By harnessing industry-leading 40nm process technology, we were able to expand the RX651 lineup by adding a product that combines a 4.5 x 4.5 mm footprint package with up to 2 MB in internal flash ROM and 640 KB of RAM. This represents a reduction of about 60% as compared to the 7.0 x 7.0 mm footprint of the smallest product in the RX651 lineup so far, enabling us to meet market needs with more flexibility. Our lineup covers a wide range, with internal flash ROM from 512 KB to 2 MB and RAM of 256 KB or 640 KB. The 64-pin small footprint package products are pin compatible across all memory configurations which helps customers to create a product lineup based on a platform using common component and board design.

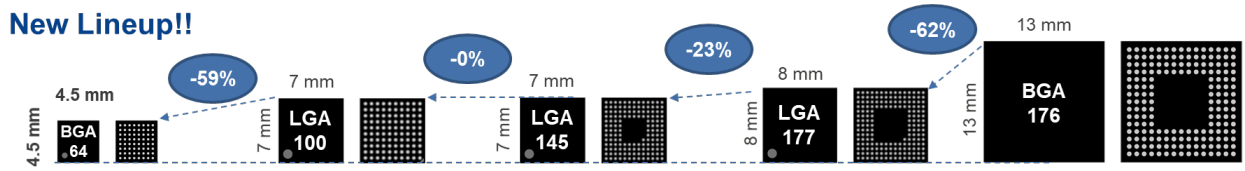

Figure 1: Small footprint package of RX651 64pin BGA

Root of Trust in Embedded System

When developing embedded systems, implementing security functions in hardware and software generally requires human development resources skilled in these aspects, and costs tend to present another hurdle. Furthermore, getting end users to appreciate the value of security is difficult. In the case of applications where security functions are clearly of high importance, such as for financial transactions and handling of confidential information, strong

security is recognized as added value by the market, so that development resources and costs are usually allotted aggressively. In such markets, the use of a dedicated chip to achieve strong security has been the usual approach.

In recent years, the spread of IoT has prompted more and more manufacturers to consider security implementations even for devices that conventionally were not connected to a network. However, due to a lack of experience with security and the fact that manufacturers of devices tend to be familiar with conventional microcontrollers, implementing strong security with a general-purpose microcontroller represents a logical approach. It therefore has become a requirement for edge device development.

Also, in the case of IoT devices connected to a network, there is a possibility that security is not assured in the cloud or server, or in a gateway or access point serving as a relay point for data transmission and reception. Therefore, IoT devices that are endpoints need to have integrated security. In order to realize this, the endpoint should have a Root of Trust component which enables the device itself to ensure that operations remains secure.

The RX651 microcontroller implements Root of Trust in hardware with a Trusted Secure IP(TSIP) feature that protects key data from leaks, and memory protection functions that can protect authorized programs from falsification.

The RX651 versions with 1.5 MB and 2 MB of flash memory integrate the (TSIP) as dedicated hardware IP for managing encryption keys, thereby preventing unauthorized access to the keys, which are also concealed by indexing for safe storage in the internal ROM.
Furthermore, the memory protection functions in all RX651 products allow the use of area protection for internal flash memory. This ensures that code stored in a specific memory area cannot be rewritten externally. Because the code that detects malicious code can itself be protected in this way, full security can be realized.

The RX651 products with TSIP lineup do not have to rely on a dedicated security chip. Strong security can be established using the functions and features of the TSIP hardware on the general-purpose microcontroller itself.

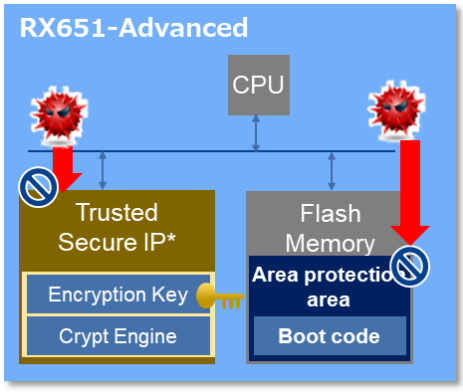

Figure 2: Root of Trust realized by Trusted Secure IP and area protection

The Trusted Secure IP of the RX651 not only supports common key cryptographic methods such as AES and 3DES but also public key cryptographic RSA required for SSL/TLS communication. Encrypted communication as required for connection to various cloud services can be implemented on a hardware basis, which enables high throughput without increasing the CPU load.

Easy Updating of Firmware

The capability for firmware updates via the network can be considered an essential aspect of IoT devices, making it possible to add new functions, apply bug fixes, and enhance the security of products after market launch. Constantly evolving methods for cyber attacks may make it necessary to apply patches to existing products. With conventional microcontrollers, firmware updates are usually performed by downloading the new firmware to a dedicated backup memory area and executing a dedicated updater. Besides requiring the controller to provide separate backup memory, this approach also makes it necessary to stop the system while downloading and applying the update. It is therefore desirable to implement the backup area in the integrated memory and enable downloading in the background.

The 2 MB and 1.5 MB Flash memory versions of the RX651 provide a Dual Bank function and support background operation (BGO). It is therefore possible to realize firmware updates with the internal flash memory only without having to stop the system. The Dual Bank function can serve to divide the internal flash memory into two banks, one for execution and a temporary area for downloading the firmware. The BGO function allows code processing in the execution area while also receiving the new firmware from the communication interface and writing it to the temporary area. When the background writing process is completed, the execution area switching register is set and a reset is performed to start running the new firmware. The boot sequence can include a step for checking the firmware for corruption, making it easy to revert to the backed up old firmware if necessary.

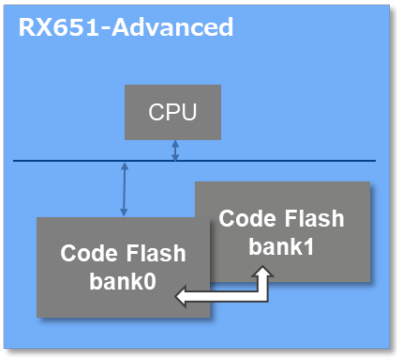

Figure 3: Dual Bank flash function

Conclusion

Features that are desirable in modules for IoT applications, such as small footprint, high memory capacity, security, and firmware update capability are all realized on a single chip in the RX651 64-pin package, with selectable versions up to 2 MB ROM and 640 KB RAM to suit the scale of the respective application. This makes the product an ideal microcontroller for configuring IoT devices without incurring cost increases.