

# RL78/G1D

## Bluetooth® Beacon Applications

### Summary

An increasing number of systems and products are being built around applications that harness the capabilities of Bluetooth low energy beacons.

This Application Note presents examples of applications that use beacons and explains the requirements for beacon devices, the formats of beacon transmission data, and how beacons are implemented.

### Target Device

RL78/G1D (R5F11A), RL78/G1D module (RY7011)

### Related materials

Name	Document No.
RL78/G1D Beacon Stack User's Manual	R01UW0171
RL78/G1D Beacon Stack Basic Operation Sample Program	R01AN3045
RL78/G1D Beacon Stack Connecting and Updating Beacon Data Sample Program	R01AN3313

## Contents

1. Beacon Applications .....	3
1.1 Point-of-interest (POI) information.....	3
1.1.1 Coupon distribution .....	3
1.1.2 Indoor positioning service.....	4
1.2 Tracking.....	5
1.2.1 Tracking people.....	5
1.2.2 Locating lost objects.....	6
1.3 Sensor devices .....	6
1.3.1 Sensors installed in confined spaces .....	6
1.3.2 Control of equipment.....	7
2. Requirements for Beacons .....	8
2.1 Low power consumption.....	8
2.1.1 Frequency of battery replacement.....	8
2.1.2 Battery-free use .....	9
2.2 Communication distance .....	10
2.2.1 Precision of location measurement .....	10
2.2.2 Communication range .....	11
2.3 Transmission of various types of data.....	11
2.3.1 Precision of location measurement .....	11
2.3.2 Sending data on the same channel.....	11
3. Beacon Formats .....	12
3.1 Sending ID data.....	12
3.1.1 iBeacon.....	12
3.1.2 Eddystone-UID .....	13
3.2 Sending sensor data .....	14
3.2.1 Eddystone-TLM .....	14
3.2.2 Custom formats .....	15
3.3 Other formats.....	16
3.3.1 URL (Eddystone-URL) .....	16
4. Implementing Beacons .....	17
4.1 Broadcast (advertising) .....	17
4.2 Observer (Scan).....	18
5. Conclusion.....	19
Revision History.....	20

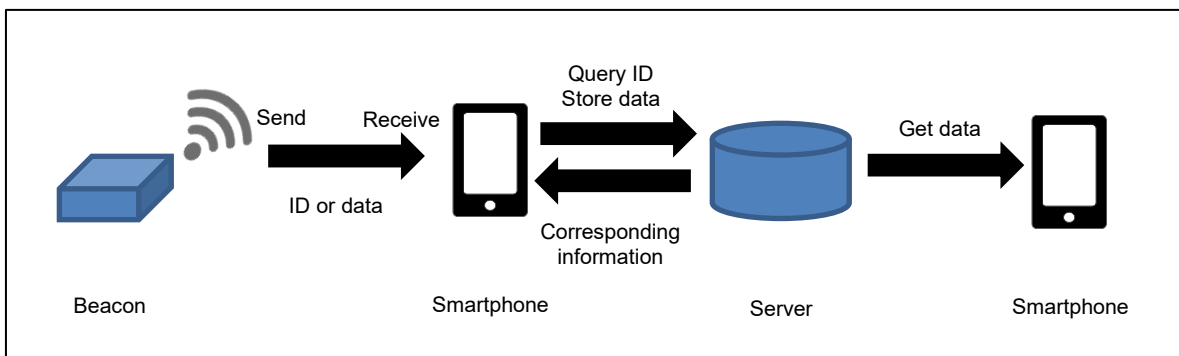
## 1. Beacon Applications

Bluetooth low energy beacons are devices that broadcast using the Bluetooth low energy technology standard. The term “broadcast” refers to a network topology used to provide one-to-many (1:m) device communication. The beacon transmits a signal encoding small amounts of data over a radius of several tens of meters at intervals ranging from every few milliseconds to every few seconds.

Because beacons are optimized for local information sharing, they are used for such applications as providing point-of-interest (POI) information, providing directions, tracking people, and locating lost objects. Beacons can also be used to transmit sensor information from hard-to-reach locations.

Beacons work by broadcasting a unique ID. Once a smartphone receives a beacon’s ID data, it can query a server for information corresponding to that ID, retrieve the information, and save the data to a server. Data stored on the server can also be retrieved from other smartphones.

**Figure 1. How beacon applications work**



### 1.1 Point-of-interest (POI) information

POI systems, which associate information with a specific location, are used to point out landmarks or indicate the locations of stores and products. Anything on a map can be set as a POI.

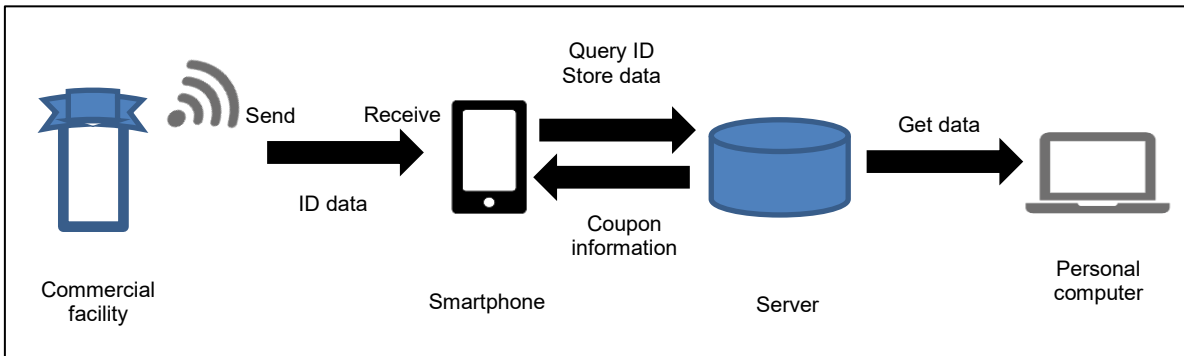
#### 1.1.1 Coupon distribution

When you approach a store or other commercial facility, product or coupon information can be delivered to your smartphone, for example through a social network application.

When your smartphone receives the ID data of the beacon installed in a commercial facility, the smartphone queries a server using some other (non-Bluetooth) communication method to retrieve the product or coupon information corresponding to that ID.

Meanwhile, the ID data stored on the server provides information about the behavior of the smartphone user, which can be useful for marketing.

Figure 2. Coupon distribution

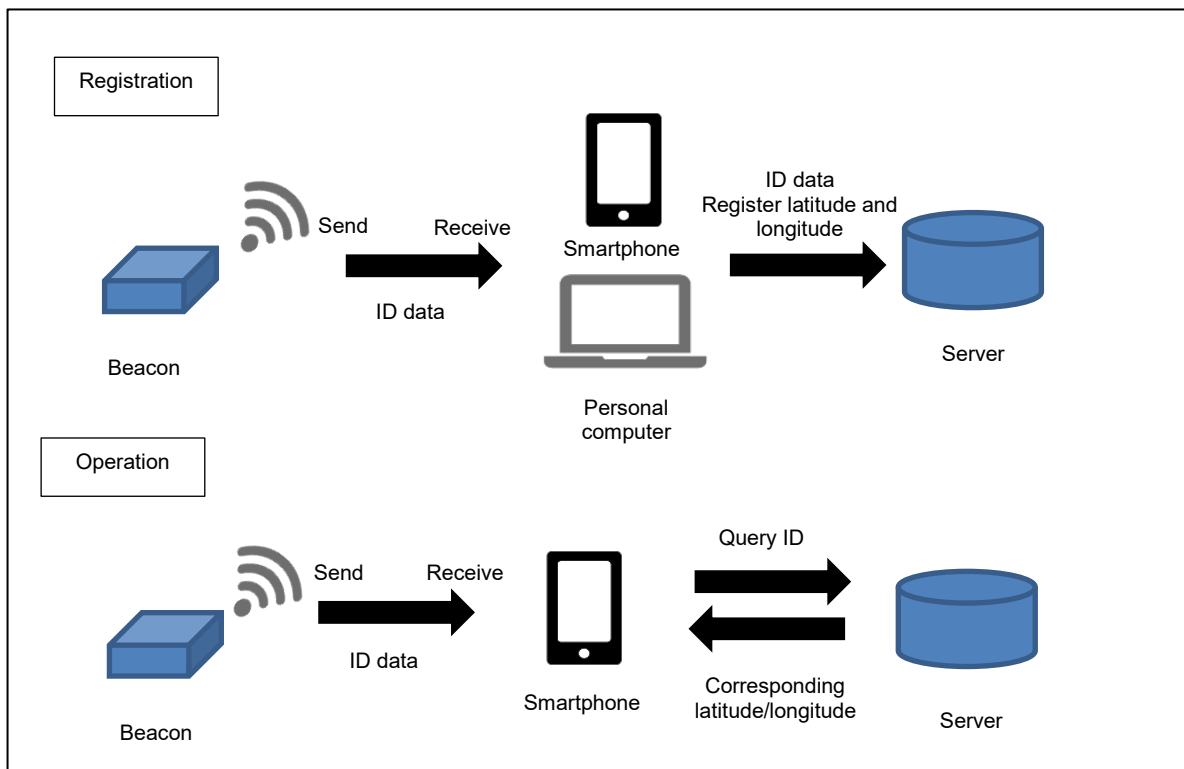


1.1.2 Indoor positioning service

In general, GPS is used as an outdoor positioning technology. Beacons, on the other hand, are used for spot positioning indoors, out of the reach of GPS signals. Currently, mechanisms are being put into place to link beacon ID data to location information. These applications require low-power beacon devices.

The indoor positioning service registers the beacon’s ID data and the latitude and longitude of the location where the beacon is installed. During actual operation, when a smartphone receives a beacon’s ID data, it queries the server for the corresponding latitude and longitude, which it uses to display the location in a mapping app.

Figure 3. Indoor positioning service



## 1.2 Tracking

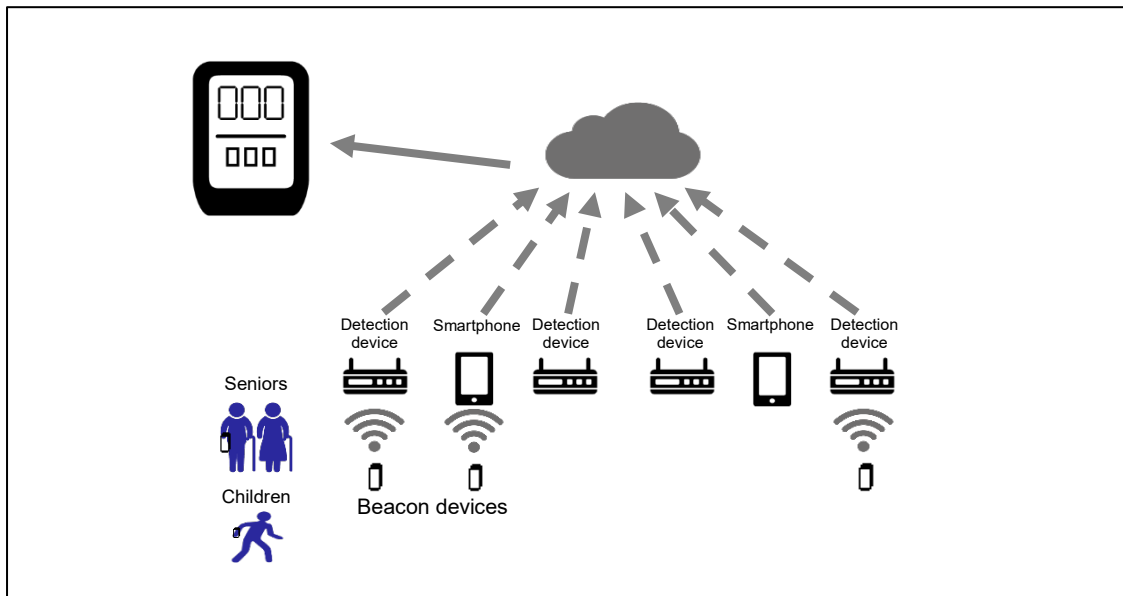
Tracking is used to detect the movements of people and objects.

### 1.2.1 Tracking people

An example application is the tracking of elderly people or children outfitted with beacon devices. Detection devices are installed in facilities or important locations in order to receive radio signals from these beacon devices. Examples of installation locations include schools for children, community centers for the elderly, homes, and public places. In other cases, volunteers in a region may install a special application to receive beacon ID data on their smartphones. The beacon ID data received by the detection device or smartphone is stored on the server along with the device's location information.

The ID data and location information stored on the server can be displayed on the smartphone mapping apps of a restricted set of relevant users. This makes it possible to use the location information to track the movements of the individuals in possession of the beacon on monitoring devices.

Figure 4. Tracking people



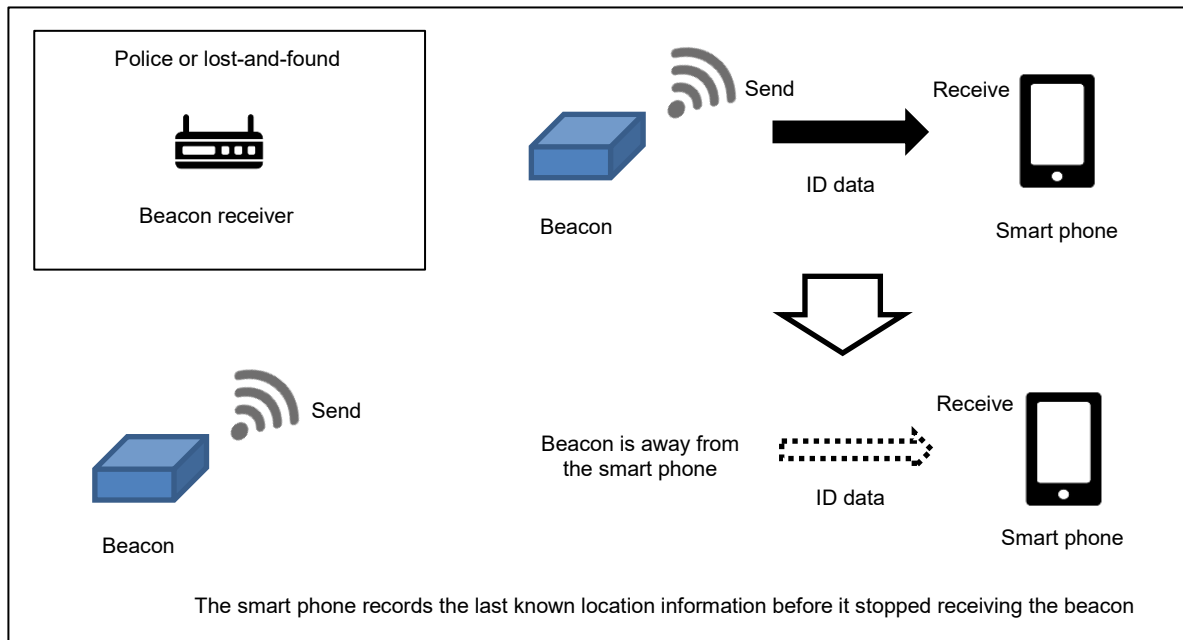
### 1.2.2 Locating lost objects

To locate lost objects, beacon devices are attached to items you do not want to lose. A smartphone application is used to receive the beacon radio signals as needed.

The smartphone records the last known location information before it stopped receiving from the beacon. This tells you where and how long ago the beacon device was last in the proximity of your smartphone.

Furthermore, if there is a beacon receiver at the police station or the lost-and-found, it will receive the beacon's ID data and store it on the server. If the item you are looking for is turned in as a lost item, you will know that its beacon device is now at the lost-and-found based on the beacon's ID data.

**Figure 5. Finding lost objects**



### 1.3 Sensor devices

Another application of beacons is to enable information from sensor devices, such as temperature data, to be broadcast to a large number of people in an open manner. For example, sensors can be placed in confined or hard-to-reach locations where conditions are difficult to check.

#### 1.3.1 Sensors installed in confined spaces

Beacons can be used to report meter readings from confined spaces or to notify users when filters need to be changed. These kinds of applications require operating under low power consumption.

To reduce power consumption, you can report beacon data only at fixed times, for example when a meter's value changes or when a filter needs to be changed.

If it is necessary to transmit beacon signals at fixed intervals to confirm normal operation, operation at lower power consumption can be achieved by increasing the length of the interval.

### 1.3.2 Control of equipment

Beacons are also used to control equipment. Sensors and other instruments linked to the equipment transmit their data over beacons. The beacon data is monitored to ensure that the equipment is running in a manner that is consistent with the observed data. Table 1 provides examples of sensor applications and how they are used.

**Table 1. Sensor applications**

Category	Application	Purpose
Home Appliance	Air conditioner	Remote temperature and humidity monitoring
Home Appliance	Air purifier	Thorough monitoring of air pollution
Home Appliance	Electric kettle	Notification of boiling by a heat sensor; detection of when boiling vibrations stop
Home Automation	Security	Detecting intruders (glass breaking)
Smart Home	Awnings	Opening and closing based on rain, brightness
Smart Home	Lighting (outdoor lights)	Switching on and off based on brightness
Smart Home	Crime prevention systems	Reporting from motion sensors
Building Automation	Lighting, air conditioning	Controlling various systems based on motion sensors
Building Automation	Doors	Opening and closing by sound
Hobby	Irrigation (gardening)	Watering by monitoring soil condition and outdoor temperature
Hobby	Pet monitoring	Pet status notifications
Hobby	Dog walking products	Monitoring your dog's pulling force

## 2. Requirements for Beacons

Beacons have requirements related to low power consumption, communication distance, and how data is transmitted.

### 2.1 Low power consumption

Beacon transmitters typically run on coin cells or small batteries. In order to keep sending radio signals at regular intervals, they are required to operate under the lowest possible power consumption.

#### 2.1.1 Frequency of battery replacement

Preparing and installing replacement batteries for battery-operated applications is cumbersome, so it is desirable to save as much time and effort as possible. It is therefore important to be able to estimate battery life to know when batteries should need to be replaced.

The formula below lets you calculate battery life based on the battery's energy rating and power consumption by the application. Note also that when power leakage is taken into account, the amount of usable energy in a battery is generally only about 80% of the total amount.

$$(battery-power [Wh] * 0.8 / average-application-power [W]) / 24 [h] = battery-life-in-days [days]$$

For example, if the capacity of a CR2032 coin cell is 220 mAh, the power will be 660 mWh at 3 V. If the average current of a Bluetooth low energy device is 20 µA, then at a voltage of 3 V the average power will be 60 µW = 0.06 mW.

$$(660 mWh * 0.8 / 0.06 mW) / 24 \approx 366 \text{ days}$$

In this case, the calculation shows that the battery should last for about one year. If you can change the interval between transmissions of the beacon device to reduce the average power, you can reduce the frequency of battery replacement.

For reference, the capacities of the principal battery types are as follows:

CR2032 coin cell: 220 mAh @3 V; AAAA alkaline battery: 800 mAh @1.5 V; AAA alkaline battery: 1,100 mAh; AA alkaline battery: 2,400 mAh.

Use this information when selecting the battery to be used. However, note that battery capacity will vary depending on the manufacturer, and voltage drops during use also must be taken into account.

The current consumption of the RL78/G1D can be estimated using the Web Simulator current consumption calculation tool.

Web Simulator current consumption calculation tool:

<http://resource.renesas.com/resource/lib/eng/websimulator/index.html>



### 2.1.2 Battery-free use

The ultimate way to reduce battery replacements is to go battery-free.

Of course, battery-free operation still requires a source of energy. Battery-free energy sources include vibration, acceleration, impact, load, and sunlight.

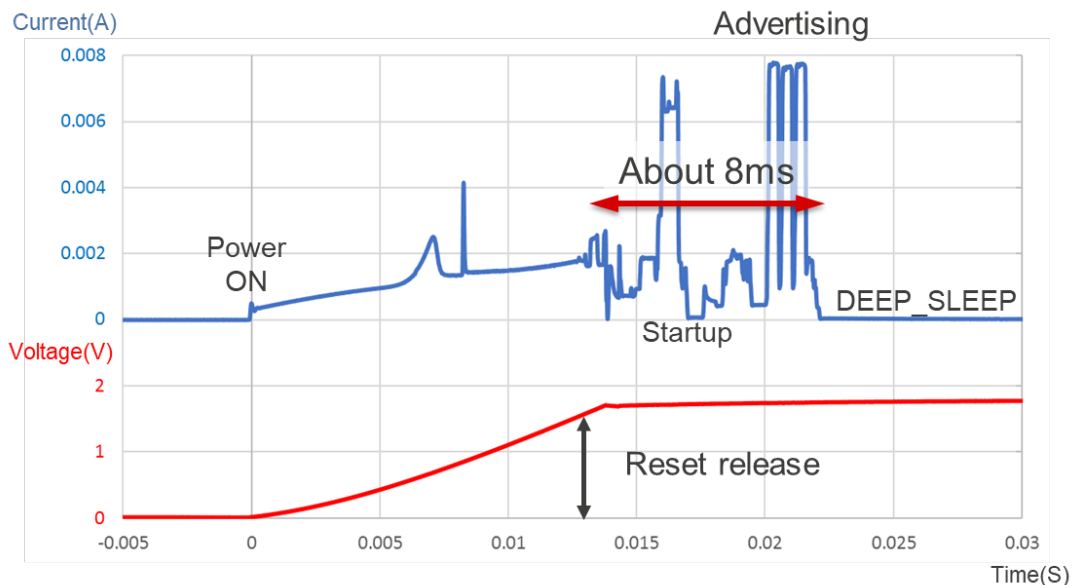
These energy sources generate different voltages and may be AC or DC depending on the generation method. To make it usable, the micro-energy is rectified into direct current and charged to a capacitor. The capacitor should be inexpensive with small capacitance. Beacons running with small capacitors need to start quickly with low power usage.

The figure below shows an example of the electric current waveform from the power supply of a beacon that is transmitting data. The microcontroller starts, performs initialization in a short period of time, and sends a beacon signal. The microcontroller then goes into sleep mode to reduce power consumption.

In the case of photovoltaic or other energy sources that generate power continuously, power during the sleep mode is charged to the capacitor up to the level at which beacon data can be transmitted, and then the transmission is executed after a fixed interval. As the figure shows, if the amount of power required to transmit a packet is small, the beacon data can be sent at shorter intervals.

In the case of impact energy or other sources that generate power all at once, at each impact it is necessary to start the MCU, perform initialization, and initiate transmission of the beacon signal. Transmission of the beacon ends when the energy source is depleted, causing the voltage to drop. In this case, it is useful to send many beacons at short intervals so that as much beacon data as possible is transmitted to the receiver.

**Figure 6. Example current waveform**



## 2.2 Communication distance

The attenuation characteristics of radio waves can be used to estimate the distance between the transmitter and the receiver for the purpose of using a beacon to measure the location of a person or object. Also, for precise location identification, communication at close range may be required.

### 2.2.1 Precision of location measurement

The 2.4-GHz frequency band used by beacons is also used by many other types of devices. Because the Bluetooth low energy communication standard has relatively weak transmission power, it is necessary to be aware of radio interference and other characteristics of radio waves.

In general, radio waves attenuate at a rate inversely proportional to the square of the transmission distance. When there are no obstacles, the radio waves propagate forward. When there are obstacles, phenomena such as reflection and absorption may occur, depending on the materials in the path of the waves. Lower frequencies can go around obstacles. Radio waves can be strengthened or weakened when waves of similar frequencies are present.

The 2.4-GHz frequency band is particularly vulnerable to such phenomena as reflection and absorption, depending on the materials in the path of the waves. The communication distance will therefore vary depending on the environment.

The strength of reception (RSSI = Received Signal Strength Indicator) is expressed by the equation shown below. The communication distance curve depends on the propagation environment coefficient  $n$ , which indicates the current status of the radio waves.

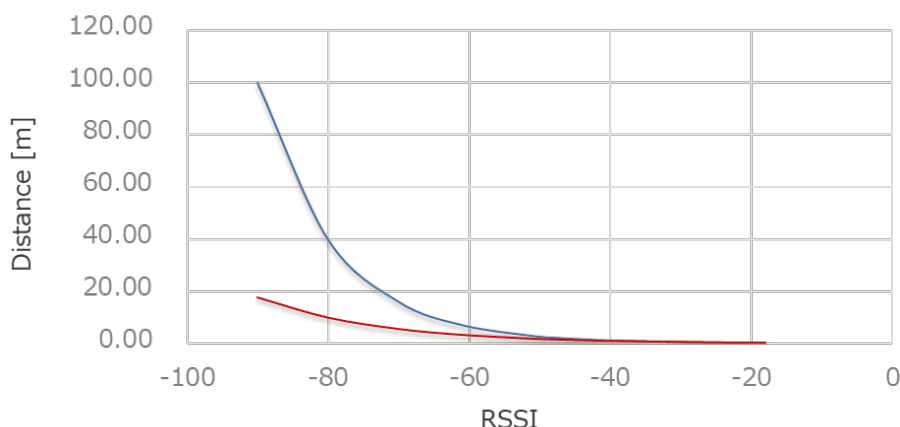
$$RSSI = TxPower - 40 - (10 * n) * \log_{10}(Distance), \text{ where } n \text{ is the propagation environment coefficient}$$

$$Distance = 10^{(TxPower - RSSI - 40) / (10 * n)}$$

In the figure below, the blue line (top) indicates a good propagation environment of  $n = 2.5$ , and the red line (bottom) indicates a bad propagation environment of  $n = 4.0$ . When the RSSI values are small, the corresponding distance calculations differ significantly.

For this reason, the iBeacon protocol categorizes distances into three ranges: Immediate (i.e., extremely close), Near, and Far. By understanding these principles, you can estimate the approximate distance of transmission.

Figure 7. RSSI vs. distance



## 2.2.2 Communication range

When using beacons for POI (point-of-interest) services, you may want to limit the range of communication or you may want to communicate over the widest possible range.

If you want to limit the communication range, one way is to decrease the transmission power. It is also important to verify the communication range during installation, taking into account factors such as the height of the installation and the orientation of the antenna.

## 2.3 Transmission of various types of data

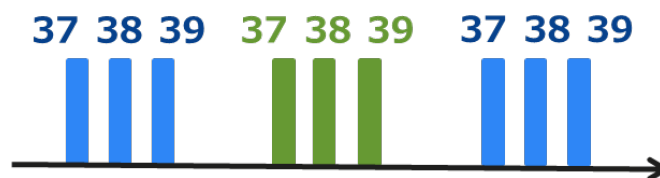
Beacons are being used in an increasing variety of applications. This is leading to an increasing need to handle multiple types of data.

### 2.3.1 Precision of location measurement

The types of data transmitted by beacons can include ID data, sensor data, and data in custom formats. Beacons can therefore be used to send multiple types of data, not just data of a single type.

Furthermore, because there are limits on the size of the data that a beacon can send, data that is too large can be split into multiple packets.

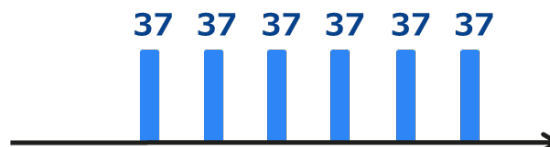
Figure 8. Sending different data



### 2.3.2 Sending data on the same channel

The sending and receiving sides typically switch channels to avoid conflict with other radio signals. However, in cases where the receiver uses a proprietary specification, you can increase the accuracy of communication by fixing the channels on both the sending and receiving sides.

Figure 9. Sending data on the same channel only



### 3. Beacon Formats

#### 3.1 Sending ID data

Transmission of ID data in beacon formats works by assigning unique IDs to places, things, and people, and then transmitting that ID data in order to make the application work.

There has been widespread adoption of the iBeacon™ format, which was introduced early in the development of beacon technology and was adopted for the iPhone®.

##### 3.1.1 iBeacon

iBeacon, a format defined by Apple, is a trademark of Apple, Inc. Since it was announced by Apple in 2013, iBeacon has become synonymous with beacon technology.

In iBeacon format, the following data is transmitted:

- UUID
- Major
- Minor
- Tx power

UUID is a 128-bit identifier. It is used by the app's beacons as a shared identifier. Major and Minor are each 16-bit data values used to uniquely identify a beacon. A large number of combinations can be generated by combining one UUID with different Major/Minor values. Tx power is an 8-bit value indicating the transmission power at a particular distance from the beacon. For more information, see the Proximity Beacon Specification. By agreeing to the license terms, you can obtain iBeacon from the following website:

iBeacon

<https://developer.apple.com/ibeacon/>

The format of the header part in the iBeacon format is shown in Table 2.

**Table 2. iBeacon format**

Byte(s)	Value	Field	Description
0	0x02	Length	2 bytes
1	0x01	AD Type	<<Flags>>
2	0x06	AD Data	LE General Discoverable Mode (bit 1) BR/EDR Not Supported (bit 2)
3–29			Please Proximity Beacon Specification.

### 3.1.2 Eddystone-UID

Eddystone is an open specification defined by Google. It was announced by Google in 2015, after the debut of iBeacon. Eddystone-UID is a format for sending unique IDs. In Eddystone-UID format, the following data is transmitted:

- Namespace ID
- Instance ID
- Tx power

Namespace ID is an 80-bit name ID. This ID is generated by using the first 10 bytes of your FQDN hashed by SHA-1. A recommended alternative to this method is to generate the UUID as above and then remove bytes 5–10 from the UUID. Instance ID is a 48-bit instance identifier. This ID area can be used in the same way as the 4 bytes of Major/Minor defined in iBeacon, but extended to 6 bytes. Tx power is an 8-bit value indicating the transmission power at 0 meters from the beacon. The Eddystone-UID format is shown in Table 3.

**Table 3. Eddystone-UID format**

Byte(s)	Value	Field	Description
0	0x02	Length	2 bytes
1	0x01	AD Type	<<Flags>>
2	0x06	AD Data	LE General Discoverable Mode (bit1) BR/EDR Not Supported (bit2)
3	0x03	Length	3 bytes
4	0x03	AD Type	<<Complete List of 16-bit Service Class UUIDs>>
5, 6	0xAA, 0xFE	AD Data	Eddystone (0xFEAA)
7	0x17	Length	23 bytes
8	0x16	AD Type	<<Service Data>>
9, 10	0xAA, 0xFE	Service UUID	16-bit Service UUID, Eddystone UUID (0xFEAA)
11	0x00	Frame Type	UID
12	0xFF	Tx Power	Calibrated Tx Power at 0 m
13–22		Namespace ID	Namespace ID, 10 bytes
23–28		Instance ID	Instance ID, 6 bytes
29, 30		RFU	Reserved for future:0x00, 2 bytes

The details of the specification are described on the following sites:

Google Beacon Platform

<https://developers.google.com/beacons/eddystone>

Eddystone-UID

<https://github.com/google/eddystone/tree/master/eddystone-uid>

## 3.2 Sending sensor data

### 3.2.1 Eddystone-TLM

Eddystone is an open specification defined by Google. Eddystone-TLM is a format for sending the battery voltage, temperature, and other data. In Eddystone-TLM format, the following data is transmitted.

- Battery voltage, 1 mV/bit (2 bytes)
- Beacon temperature (2 bytes)
- Advertising PDU count since power-on or reboot (4 bytes)
- Time since power-on or reboot (4 bytes)

Eddystone-TLM defines unencrypted and encrypted specifications. The unencrypted Eddystone-UID format is shown in Table 4.

**Table 4. Eddystone-TLM format**

Byte(s)	Value	Field	Description
0	0x02	Length	2 bytes
1	0x01	AD Type	<<Flags>>
2	0x06	AD Data	LE General Discoverable Mode (bit1) BR/EDR Not Supported (bit2)
3	0x03	Length	3 bytes
4	0x03	AD Type	<<Complete List of 16-bit Service Class UUIDs>>
5, 6	0xAA, 0xFE	AD Data	Eddystone (0xFEAA)
7	0x10	Length	16 bytes
8	0x16	AD Type	<<Service Data>>
9, 10	0xAA, 0xFE	Service UUID	16-bit Service UUID, Eddystone UUID (0xFEAA)
11	0x20	Frame Type	TLM
12	0x00	TLM Version	
13, 14		VBATT	Battery voltage, 1 mV/bit
15, 16		TEMP	Beacon temperature
16–19		ADV_CNT	Advertising PDU count
20–23		SEC_CNT	Time since power-on or reboot

All multi-byte values are big-endian.

The details of the specification are described on the following site:

Eddystone-TLM

<https://github.com/google/eddystone/tree/master/eddystone-tlm>

### 3.2.2 Custom formats

Beacon data can be transmitted in custom formats. These formats are typically used to transmit sensor data by defining a Manufacturer Specific Data type. The first two bytes of a Manufacturer Specific Data type encode a Company Identifier Code. The Company Identifier Code is a unique value assigned by the Bluetooth SIG to a member company that requests it. Check the Bluetooth SIG Web page for more information. The structure of the custom format is shown in Table 5.

You can send up to 24 bytes as custom data. This area consists of unique values that identify the sensors as well as multiple sensor data.

**Table 5. Custom format**

Byte(s)	Value	Field	Description
0	0x02	Length	2 bytes
1	0x01	AD Type	<<Flags>>
2	0x06	AD Data	LE General Discoverable Mode (bit1) BR/EDR Not Supported (bit2)
3	Max 0x1B	Length	XX bytes (Max: 27 bytes)
4	0xFF	AD Type	<<Manufacturer Specific Data>>
5, 6	0XXXXX	Company ID	Company Identifier Code: 2 bytes (0XXXXX)
7–30		Custom Data	Custom element: Max 24 Bytes

Details of the Company Identifier Code are described on the following site:

Bluetooth SIG - Company Identifier Code

<https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers>

### 3.3 Other formats

#### 3.3.1 URL (Eddystone-URL)

Eddystone is an open specification defined by Google. Eddystone-URL is a format for sending URLs, which identify Web pages. It was initiated in 2014 as part of Google's Physical Web Project. It was supported in Google Chrome for a while, but today is no longer supported. Building a service requires implementation of your own application. For details, refer to the Physical Web information on GitHub.

Beacon data is limited in size. For this reason, it is assumed that the Web page URLs will use a short URL format. Short URL creation services include Firebase Dynamic Links (FDL), Ow.ly, and Bitly. These services make it easy to create short URLs.

**Table 6. Eddystone-URL format**

Byte(s)	Value	Field	Description
0	0x02	Length	2 bytes
1	0x01	AD Type	<<Flags>>
2	0x06	AD Data	LE General Discoverable Mode (bit1) BR/EDR Not Supported (bit2)
3	0x03	Length	3 bytes
4	0x03	AD Type	<<Complete List of 16-bit Service Class UUIDs>>
5, 6	0xAA, 0xFE	AD Data	Eddystone (0xFEAA)
7	0x17	Length	23 bytes
8	0x16	AD Type	<<Service Data>>
9, 10	0xAA, 0xFE	Service UUID	16-bit Service UUID, Eddystone UUID (0xFEAA)
11	0x10	Frame Type	URL
12	0xFF	Tx Power	Calibrated Tx Power at 0 m
13	0x00	URL Scheme	URL Scheme, 1 byte: 0x00 http://www. 0x01 https://www. 0x02 http:// 0x03 https://
14–30		Encoded URL	Length 1–17

The details of the specification are described on the following sites:

Eddystone-URL

<https://github.com/google/eddystone/tree/master/eddystone-url>

GitHub Physical Web

<https://github.com/google/physical-web>



## 4. Implementing Beacons

### 4.1 Broadcast (advertising)

Renesas provides a beacon stack specialized for beacon operation.

Our beacon stack documentation is listed in Table 7. A sample program for beacon operation can be found in “Basic Operation Sample Program” (R01AN3045). The program is small, only about 15 KB in size. You can easily try it out by compiling it with the free evaluation version.

“Connecting and Updating Beacon Data Sample Program” (R01AN3313) is an Application Note that explains how to change the beacon settings using the Bluetooth low energy connection mode.

**Table 7. Beacon stack documentation**

Name	Document No.
RL78/G1D Beacon Stack User’s Manual	R01UW0171
RL78/G1D Beacon Stack Basic Operation Sample Program	R01AN3045
RL78/G1D Beacon Stack Connecting and Updating Beacon Data Sample Program	R01AN3313

The beacon stack sample program demonstrates how to experiment with beacons.

The beacon settings include hardware settings and application settings. The hardware settings include the settings listed below. These settings change the processing time at startup and the accuracy of the operation timing. You can change the settings to suit your application.

- MCU main system clock frequency
- Whether or not to receive using RF transmit/receive operation
- Whether or not to use RF-internal DC-DC converter
- RF slow clock source
- Whether or not to perform RF-internal oscillator calibration

For energy harvesting, use the settings below to shorten the startup time and achieve low power consumption. In addition, because the MCU unit is driven by the built-in LDO regulator, the lower the voltage, the lower the power. Therefore, if you want to use an external regulator and you run the MCU in LS (low-speed main) mode with a minimum operating voltage of 1.8 V, running at voltages close to 1.8 V will result in lower power consumption.

For detailed settings to help reduce power consumption, see the energy harvesting hardware settings in the “Basic Operation Sample Program” (R01AN3045).

- Reduce RF initialization time by setting the RF transmit/receive behavior to transmit-only
- Use the RF-internal DC-DC converter to reduce RF transmission current consumption
- Select the RF-internal oscillator as the RF slow clock source to reduce the oscillation stabilization wait time of the XT1 oscillator
- Switch off RF-internal oscillator calibration to reduce the oscillation stabilization wait time

The remainder of this section explains how to change the beacon data.

The application settings can be set in the program code in the form of settings for beacon and scanning behavior and initial values for beacon behavior.

In addition, you can write unique codes to designated flash memory areas for easy configuration of unique beacon behaviors. Figure 10 shows an example of setting a unique code in Renesas Flash Programmer. In

addition to various settings, you can configure beacon data as shown in the gray area. For details, see 6.2.2 “System Operation Settings” in the “Basic Operation Sample Program” (R01AN3045).

The Renesas Flash Programmer software can be used to easily configure the writing of unique codes to flash memory.

**Figure 10. Example of setting a unique code in Renesas Flash Programmer**

```

1: // -----
2: // -- System Configuration for RL78/G1D Beacon Stack Sample Program --
3: // -- Device Part Number : R5F11AGJ --
4: // -----
5: format hex
6: area user flash
7: address 0x3f400
8: size 122
9: index data
10: 000001 B39A7856341200FFA00001070009FFFFFFFFFFFFFFFFFFFFFFFFB0201060303AAFE1316AAFE10EE02676F6F2E67
6C2F3764694C5478000000001B0201060303AAFE1316AAFE10EE02676F6F2E676C2F3764694C5478000000001E1E0952656E
6573617320524C37382F47314420426561636F6E204461746100

```

## 4.2 Observer (Scan)

In order to receive beacon packets, the observer performs a scan to receive data from the beacon devices. The beacon stack sample program supports the ability to transmit the reception channel, RSSI, and the information stored in the packets via UART.

In the “Basic Operation Sample Program” (R01AN3045), UART commands are used to start and stop scanning and change the settings. The sample program also implements duplicate filtering and RSSI filtering.

- When duplicate filtering is enabled, the host is not notified about a packet if it receives the same Advertising packet again with the same device address and Advertising data as an earlier packet.
- When RSSI Filter is enabled, the host is not notified about a packet if the received Advertising packet’s RSSI is below a threshold.

The sample program supports UART in ASCII or binary format. Figure 11 shows an example of ASCII format UART send/receive in which a whitelist is set to ensure that beacon packets are received only from specific devices. By following these examples, you can easily experiment with receiving beacons.

**Figure 11. ASCII format UART send/receive example**

```

ADV_IND    RANDOM 64:1D:DB:DD:82:5E 38ch -77dBm 14byte 02011A0AFF4C001005031C2BAA92
SCAN_RSP   RANDOM 64:1D:DB:DD:82:5E 38ch -81dBm 0byte
ADV_NONCONN_IND RANDOM 16:62:C8:BF:21:9B 38ch -65dBm 31byte 1EFFF060001092002DE1062D0148983495CAB2789220F6DD875FA00E7161AB
Stop Scan :OK
wlist pub74905000531e
Add White List :OK

Start Scan :OK
ADV_IND    PUBLIC 74:90:50:00:53:1E 37ch -49dBm 16byte 0201060C09524C37382D466173743031
SCAN_RSP   PUBLIC 74:90:50:00:53:1E 37ch -49dBm 0byte
ADV_IND    PUBLIC 74:90:50:00:53:1E 37ch -49dBm 16byte 0201060C09524C37382D466173743031
SCAN_RSP   PUBLIC 74:90:50:00:53:1E 37ch -49dBm 0byte
ADV_IND    PUBLIC 74:90:50:00:53:1E 37ch -49dBm 16byte 0201060C09524C37382D466173743031
SCAN_RSP   PUBLIC 74:90:50:00:53:1E 37ch -49dBm 0byte

```

## 5. Conclusion

Bluetooth low energy beacons can be applied to a wide range of applications, enabling the development of more useful products and systems.

As noted in Section 2, “Requirements for Beacons,” beacon devices using the RL78/G1D (R5F11A) and RL78/G1D module (RY7011) support low power consumption and transmission of various types of data.

Low power consumption can reduce the frequency of battery replacement, and if you use energy harvesting technology, you can even use battery-free beacon devices that do not require battery replacement at all.

For more information about Renesas’ Bluetooth low energy solutions, please refer to the following website:

Bluetooth low energy

<https://www.renesas.com/solutions/proposal/bluetooth-low-energy.html>

**Revision History**

Rev.	Date	Description	
		Page	Summary
1.0	June.20. 2019	-	Created

# General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

## 1. Precaution against Electrostatic Discharge (ESD)

A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity.

Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.

## 2. Processing at power-on

The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.

## 3. Input of signal during power-off state

Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.

## 4. Handling of unused pins

Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.

## 5. Clock signals

After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.

## 6. Voltage application waveform at input pin

Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between  $V_{IL}$  (Max.) and  $V_{IH}$  (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between  $V_{IL}$  (Max.) and  $V_{IH}$  (Min.).

## 7. Prohibition of access to reserved addresses

Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.

## 8. Differences between products

Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

## Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
  2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
  3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
  4. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
  5. Renesas Electronics products are classified according to the following two quality grades: "Standard" and "High Quality". The intended applications for each Renesas Electronics product depends on the product's quality grade, as indicated below.
    - "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
    - "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.
- Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user's manual or other Renesas Electronics document.
6. When using Renesas Electronics products, refer to the latest product information (data sheets, user's manuals, application notes, "General Notes for Handling and Using Semiconductor Devices" in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
  7. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
  8. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
  9. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
  10. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
  11. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
  12. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) "Renesas Electronics" as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) "Renesas Electronics product(s)" means any product developed or manufactured by or for Renesas Electronics.

(Rev.4.0-1 November 2017)

## Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,  
Koto-ku, Tokyo 135-0061, Japan  
[www.renesas.com](http://www.renesas.com)

## Trademarks

iPhone® and iBeacon™ are trademarks of Apple Inc.

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

## Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:  
[www.renesas.com/contact/](http://www.renesas.com/contact/)