RYZ024

Module System Integration Guide

Contents

1. Hardware Control

1.1 Generic Rules

In this document, we assume that the product uses a RYZ024 module connected to an external host MCU.

The application is running on the external host MCU, which is the system's master. The modem is a slave.

RYZ024-based module behaves like a DCE.

There are several possible ways to connect the Module to an external host MCU using the UART interface (the physical UART port used usually is UART0):

Host		**Hardware Flow Control**	
		Supported	**Not supported**
Low power	Supported	Type 1: section 1.1.1	Type 3: section 1.1.3
	Not supported	Type 2: section 1.1.2	Type 4: section 1.1.4

This section ignores UART1. UART1 should be configured according to the application's needs. By default, UART1 is configured as an AT UART, with flow control, at 921600 bauds and RTS1 is a wake source of the module. UART1 was defined mainly to be used during manufacturing and debug. At the end of the manufacturing process, UART1 should be configured as a DCP UART and the RTS1 wake source should be disabled as explained in the *Module Manufacturing Guide*:

```
AT+CFUN=5
AT+SQNHWCFG="uart1","enable","rtscts","921600","8","none","1","dcp"
AT+SQNHWCFG="wakeRTS1","disable"
AT^RESET
```

1.1.1 Type 1: Hardware Flow Control Supported and Low Power Supported (recommended design)

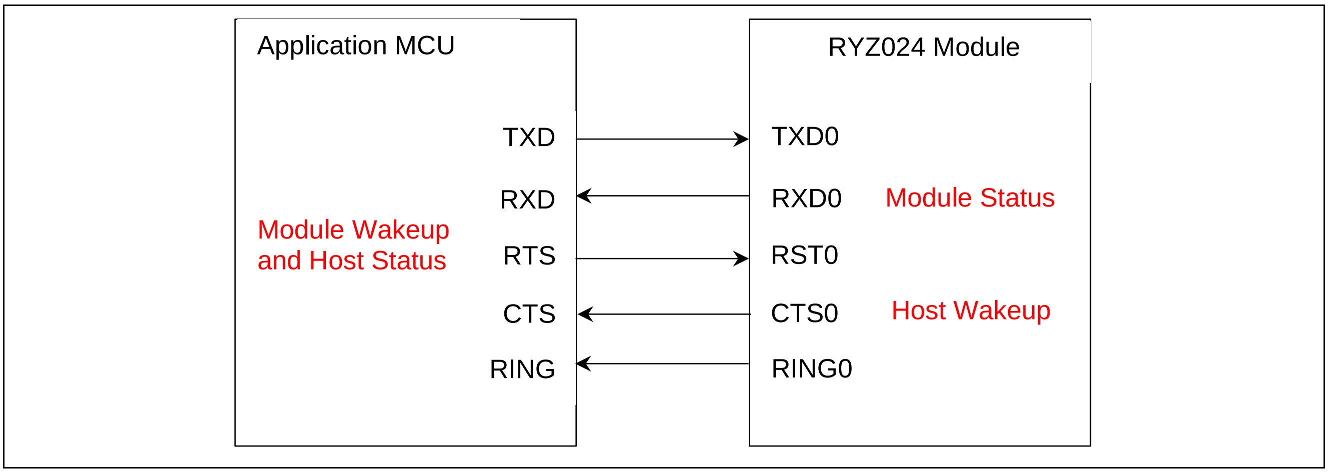


Figure 1. Hardware Flow Control and Low Power Supported

The `AT+SQNRICFG` command can be used to configure the RING function. By default, RING activation mirrors general URC events and data. The modem wakes the host up whenever URC are pending on UART0, or data are received from the network.

With this design, the system should be configured as follows:

```
AT+CFUN=5
AT+SQNIPSCFG=2,100 //Set UART timeout to 100 ms
AT+SQNHWCFG="uart0","enable","rtscts" //Enable flow control on UART0 (default configuration)
AT+SQNHWCFG="wakeRTS0","enable" //Set RTS0 as a wake source (default configuration)
AT+SQNRICFG=1,3,100 //Reduce RING timeout to 100 ms
AT^RESET
```

Please refer to the *Module Integration Guide* for the values of the customary pull ups or pull downs.

1.1.2 Type 2: Hardware Flow Control Supported and Low Power Not Supported

In this configuration, monitoring the RING line is not needed if the MCU does not use PPP or socket online mode. Hardware wiring is simpler.

Without hardware flow control:

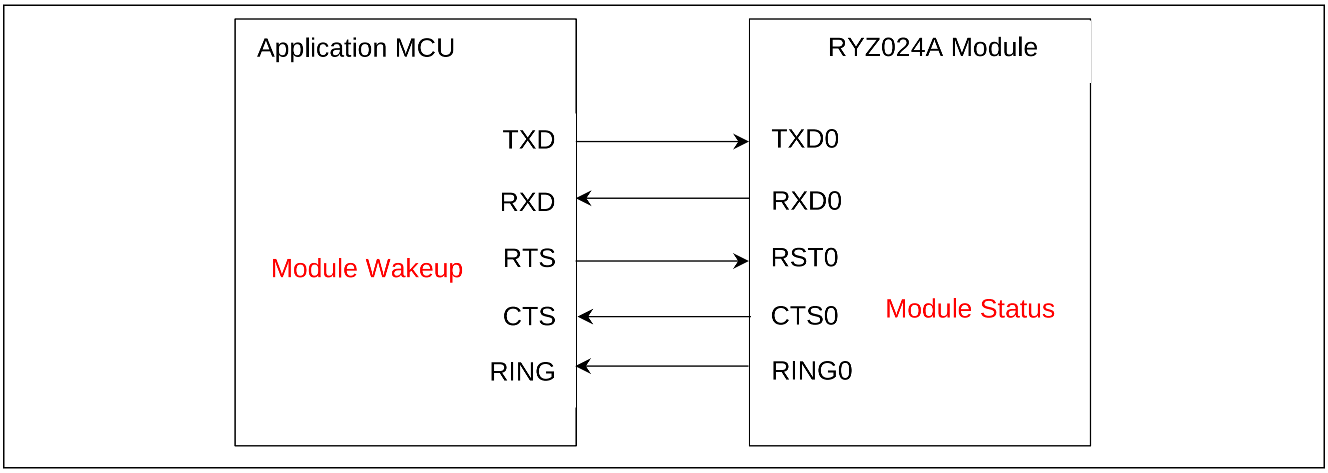


Figure 2. Hardware Flow Control with no Low Power Support

When using this paradigm, the system should be configured as follows:

```
AT+CFUN=5
AT+SQNIPSCFG=2,100 //Set UART timeout to 100 ms
AT+SQNHWCFG="uart0","enable","rtscts" //Enable flow control on UART0 (default configuration)
AT+SQNHWCFG="wakeRTS0","enable" //Set RTS0 as a wake source (default configuration)
AT+SQNRICFG=1,3,100 //Reduce RING timeout to 100 ms (optional)
AT^RESET
```

If the MCU uses PPP or socket online mode, the RING line toggles to warn of pending URCs orSMSes, prompting the MCU to resume command mode.

Please refer to the *Module Integration Guide* to check the values of the pull up or pull down that are needed on each line.

1.1.3 Type 3: Hardware Flow Control Not Supported and Low Power Supported

If the MCU does not support hardware flow control but the MCU supports low power modes, the recommended approach is to develop a piece of software to mimic the hardware flow control using two GPIOs on the host MCU

RTS0 wakes up the modem, the host MCU software must control this pin according to UART flow control protocol.

The host MCU must also handle the CTS0 pin, as the modem toggles it when sending data to the host MCU.

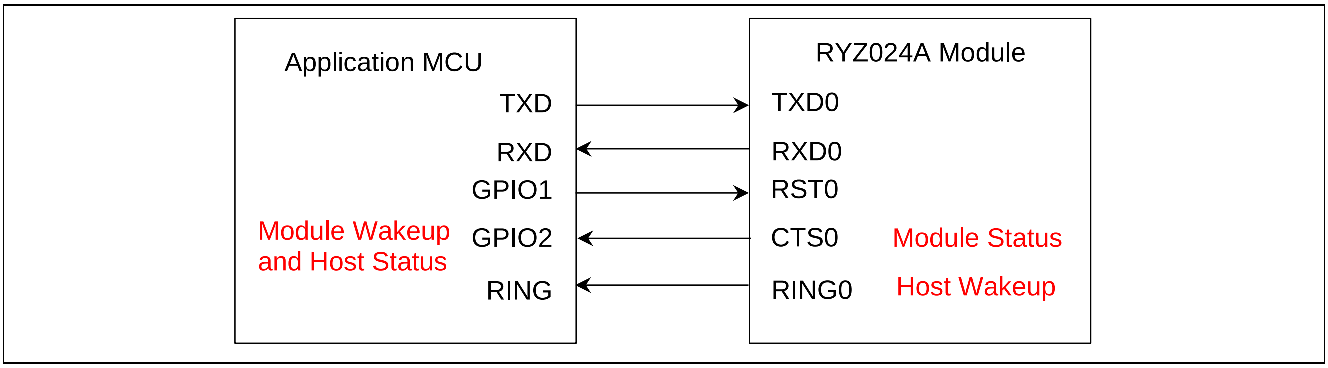


Figure 3. Hardware Flow Control Not Supported and Support for Low Power Modes

The AT+SQNRICFG command can be used to configure the RING function. By default, RING activation is triggered by general URC events and data. The modem wakes the host up whenever URC are generated on UART0, or data are received from the network.

With this design, the system should be configured as follows:

```
AT+CFUN=5
AT+SQNIPSCFG=2,100 //Set UART timeout to 100 ms
AT+SQNHWCFG="uart0","enable","rtscts" //Enable flow control on UART0
(default configuration)
AT+SQNHWCFG="wakeRTS0","enable" //Set RTS0 as a wake source (default
configuration)
AT+SQNRICFG=1,3,100 //Reduce RING timeout to 100 ms
AT^RESET
```

Please refer to the *Module Integration Guide* to check the values of the pull up or pull down that are needed on each line.

1.1.4 Type 4: Hardware Flow Control and Low Power Not Supported

If the MCU does not support hardware flow control and does not support low power modes, then the following approach can be adopted:

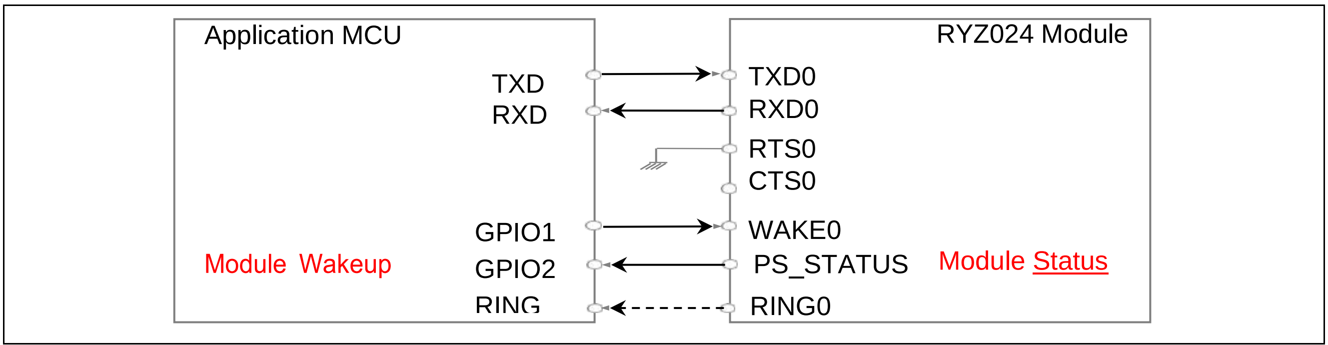


Figure 4. Hardware Flow Control and No Support for Low Power Modes

The PS_STATUS line must be connected to the MCU, which monitors it to know whether the modem is awake or needs to be woken up. Wiring the RING line is optional if the MCU does not use PPP or socket online mode.

As explained in section 1.2.3, PS_STATUS signal only indicates if the modem is awake or asleep. It does not monitor the fact that the modem is ready to receive AT commands. The host MCU must use AT polling by sending "AT+CFUN?" on the UART and wait for the "OK" response from the modem before sending any other command. It is recommended to pull down RTS0 to make sure that the UART communication is smooth. Leave CTS0 unconnected.

With this design, the system should be configured as follows:

```
AT+CFUN=5
AT+SQNIPSCFG=2,100 //Set UART timeout to 100 ms
AT+SQNHWCFG="uart0","enable","none" //Disable flow control on UART0
AT+SQNHWCFG="wakeRTS0","disable" //Unset RTS0 as wake source
AT+SQNHWCFG="wake0","enable" //Set wake0 as a wake source
AT+SQNHWCFG="ps_status","enable"  //Enable  ps_status  function  (default
configuration)
AT+SQNRICFG=1,3,100 //Reduce RING timeout to 100 ms (optional)
AT^RESET
```

Please refer to the *Module Integration Guide* for the values of the customary pull up or pull downs.

In this configuration, baud rates higher than 115200 bps on the UART connected to the MCU are not recommended. At high speeds, without flow control, it is not possible to guarantee data integrity. The MCU application should therefore handle potential data loss. The UARTs Rx/Tx FIFOs are 64-byte deep.

1.2 Signals

The host application running on the external MCU has access to the following physical interfaces of the modem:

- The UART: It is used to send AT commands in order to turn the network connectivity on or off. It can be used to perform software reset/shutdown.
- The RESETN pin of the modem: asserting this line causes a hardware reset of the modem.
- Most of the time, the MCU also controls the modem's power supply.

1.2.1 Reset Signal

See the datasheet of the module for the description of the RESETN signal. The RESETN signal is active low.

To reset the modem, the host application can use the following methods:

- UART
  - Use AT^RESET (please refer to *AT Command User's Manual*)
- RESETN
  - The application software asserts this pin to perform a hardware reset. For timing information and constraints, please refer to the Module Datasheet.
- Power supply shutdown
  - Before any power supply shutdown, a software shutdown of the modem using AT+SQNSSHDN is highly advised.
  - After sending this command, only a hardware reset using the RESET line restarts the module. Simply turning VBAT back on will not restart the device.

1.2.2 Wake source

When needed, the host application can wake the modem up by toggling any wake source. There are seven pins of the module that can be used as external wake sources: WAKE0, WAKE1, WAKE2, WAKE3, WAKE4, RTS0 and RTS1. AT+SQNHWCFG can be used to show the wake source configuration and change it. See the *Use cases with AT commands* document for more details.

1.2.3 PS_STATUS

The PS_STATUS reflects the module's current status. This signal is low when the module is in Sleep mode and goes high when the module is in active mode.

PS_STATUS can be used to supply power to antenna switches for antenna tuning or to power any component that needs to be turned on when the modem wakes up.

When no hardware flow control is used, monitoring the PS_STATUS is mandatory for proper AT command communication. Before sending any new command, the host must ensure that:

- PS_STATUS is high
- The modem AT buffer is ready. The AT buffer is ready when the host receives an `OK` response to an `AT+CFUN?` command.

The graphics below show the behavior of the PS_STATUS line with respect to the CTS0 line used when hardware flow control is on. The CTS0 line goes low when the modem is ready to receive AT commands.

- The modem wakes up from Sleep mode

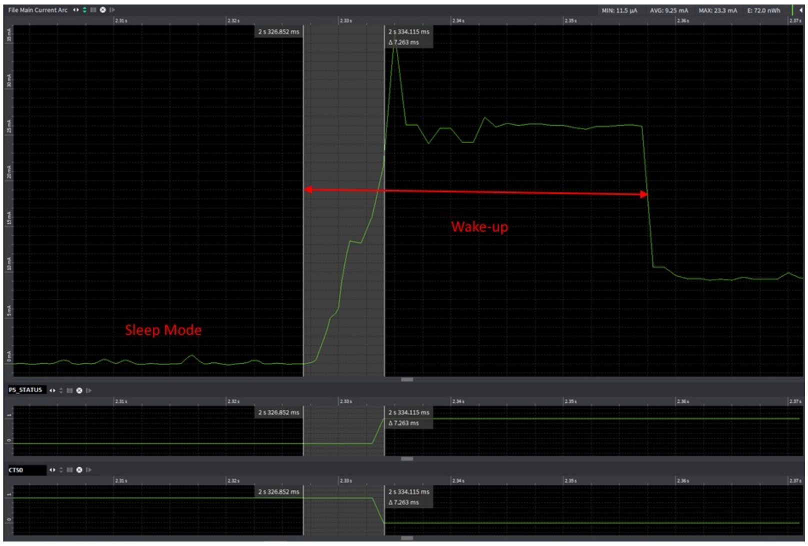


Figure 5. Modem Wakes up from Sleep Mode

In this case, PS_STATUS and CTS0 lines are asserted at the same time, the modem is ready to receive AT commands as soon as it wakes up.

- The modem wakes up from Deep Sleep mode

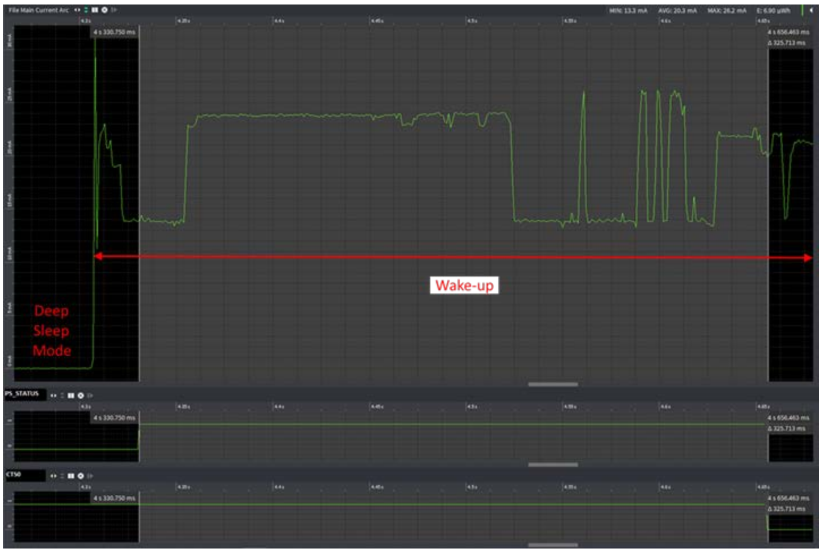


Figure 6. Modem Wakes up from Deep Sleep Mode

The PS_STATUS line becomes active 325 ms earlier than the CTS0 line. Therefore, if the CTS0 line is not monitored by the host MC, then the latter needs to perform AT polling as indicated above.

- RRC Idle

During RRC idle, the modem will go to sleep mode in between paging opportunities

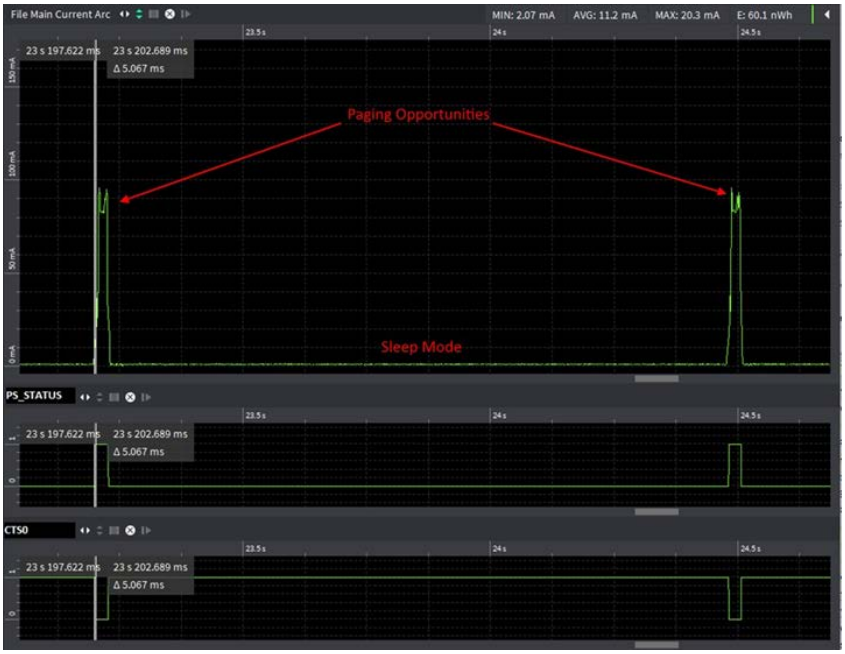


Figure 7. RRC Idle

PS_STATUS and CTS0 lines are toggling together, 5 ms after the modem wakes up to listen to the paging opportunity

- eDRX

When the modem is in eDRX mode and wakes up to listen to a paging opportunity, the CTS0 line remains high as the UART interface is never enabled. Only the PS_STATUS line toggles high then back to low, indicating that the modem woke up for a short period of time.

Figure 8. eDRX

1.2.4 Ring Line

The RING line must be monitored by the host MCU for two purposes:

- Get a URC when the UART is active and in online mode,
- Reconnect the UART to get URC and user data

By default, the RING line is active low and is activated when an URC is received on UART0. It stays low for 5 s. The RING line configuration can be modified with `AT+SQNRICFG` command. The user can decide which event toggles the RING line and how long it remains active.

The RING line toggles with every URC, whether the UART is connected or not. Following is an example of the RING line going down with an incoming URC, the duration of the RING signal being configured to 1 s in this example:

Figure 9. Ring Line Toggling

The RING line is driven high during Sleep and Deep Sleep modes.

Figure 10. Ring Line Driven High (Deep Sleep Mode)

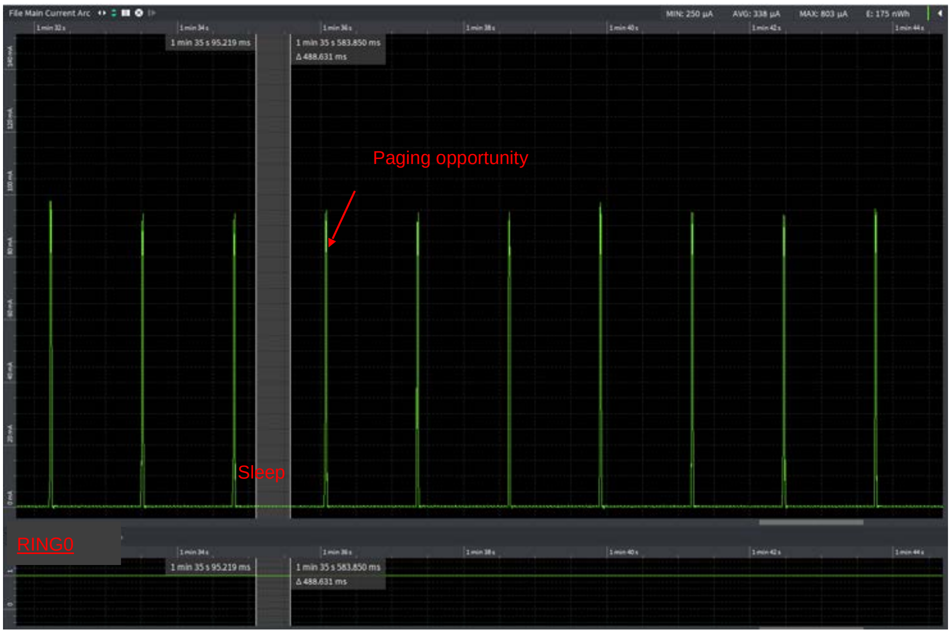


Figure 11. Ring Line Driven High (Sleep Mode)

1.3 Block Diagram

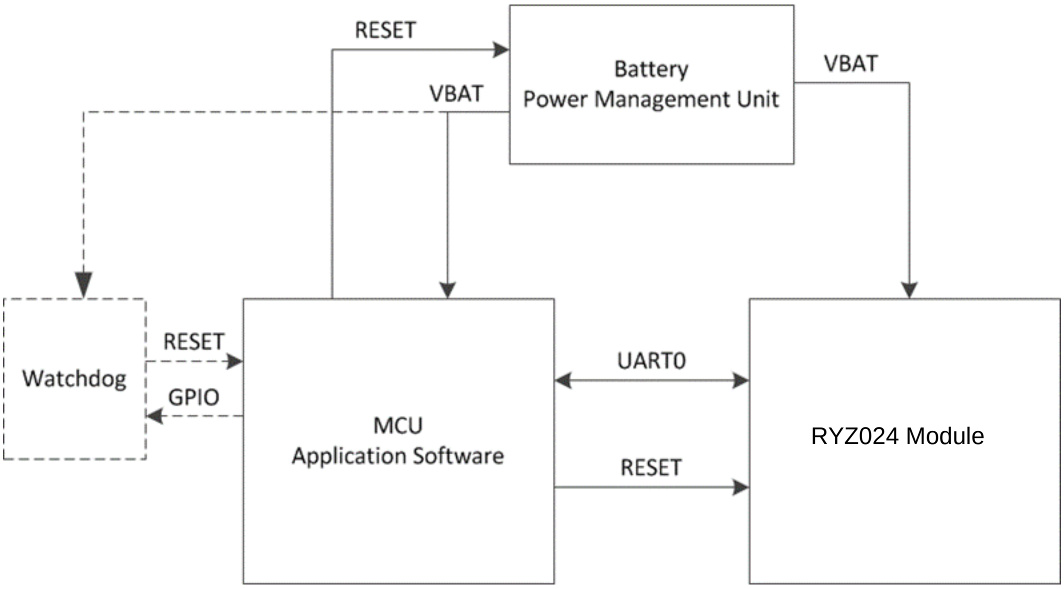


Figure 12. System Block Diagram

The power management unit (PMU) is responsible for supplying power to the different blocks. The device can be battery powered or mains power supplied. The PMU is controlled by the host application. By resetting the PMU, the application software can reset the whole platform (itself and modem). The PMU is also responsible for managing the battery charge.

The optional watchdog resets the MCU in case it detects a deadlocked situation. The application software regularly resets the watchdog before it runs out to avoid unnecessary resets.

- The timer value of the watchdog must be compatible with the low power consumption constraints of the system.
- As an example, for device entering PSM mode, the watchdog timer must be higher than the longest value of the PSM timer.

Please note that the modem itself has its own hardware watchdog

2. Software Integration

The application software running on the MCU controls the modem (including performing network attachment), exchanges data with servers, upgrades firmware and so on.

Other operations not related to LTE connectivity are not in the scope of this document.

2.1 AT Parser Generic Rules

The host MCU interacts with the RYZ024 modem through AT commands.

At boot, the modem sends a +SYSSTART URC it is ready to process AT commands. Any AT command sent to the modem before the reception of the +SYSSTART URC is discarded.

By default the modem starts in state CFUN=0 (minimum functionality). It does not try to attach to the network until the host MCU sets it in CFUN state to 1 (full functionality).

AT command are handled sequentially by the modem. The host MCU must not send a new AT command before receiving the acknowledgement for the previous one. There are two types of AT commands:

- Synchronous
  - The AT command returns a result
  - This can take several seconds
  - The execution time of an AT command often depends on the network, and therefore it is not possible to set a timeout for these. The host MCU should implement its own AT command timeout as explained in section 2.2.4.1, AT Commands Timeout that follows.
  - During the execution of a synchronous command, no other commands or URC can be processed. All incoming traffic is delayed until the command ends.

- Asynchronous
  - The AT command returns within 300 ms
  - The result is communicated later using a URC (Unsolicited Result Code)
  - The host MCU has to be ready to receive the URC at any time. The RYZ024 module activates the RING line of the AT UART to notify of pending URCs.

2.1.1 AT Command Syntax

All AT commands supported by RYZ024 modules comply with 3GPP TS 27.005-11.0.0 section 4.

2.1.1.1 Command Line

There are three types of commands:

- Write Commands

Syntax	Description
AT<cmd>	Basic command, no '+' prefix
AT<cmd>=xx	Basic command with sub parameter
AT+<cmd>	Extended command (prefixed with '+')
AT+<cmd>=,,xx	Some sub parameters may be omitted
AT^<cmd>	Some private AT commands use '^' instead of '+', e.g. AT^RESET

- Read Commands

Syntax	Description
AT+<cmd>?	To check current sub parameter values

- Test Commands

Syntax	Description
AT+<cmd>=?	To check possible sub parameter values

AT commands are terminated as follows:

Syntax	Description
`<CR>`	Command line termination character (settable)
`AT+<cmd1>;AT+<cmd2>`	Semicolons. If the first command generates an URC, it may arrive during the execution of the second command.

2.1.1.2 Responses

There are four types of responses that may be issued by the DCE:

- Information Text

Syntax	Description
`[+<cmd>: ]free text<CR><LF>`	Response to Write command. Multi-line response is possible. Each line has the same format.
`+<cmd>: (0-3),(0,1),(0-10,15),("aa","bb")<CR><LF>`	Response to Test command

- Result Codes

Syntax	Description
`<CR><LF><result code><CR><LF>`	Verbose result code (**ATV1,** default)
`<numeric><CR>`	Terse result code in **ATV0**

- Intermediate Result Code
  An intermediate result code reports on the progress of a DCE's action.

  For example, after successfully opening a socket connection in command mode using AT+SQNSD, the DCE sends the intermediate result code CONNECT.

  The DCE then moves from command state to online data state and does not accept AT commands anymore.

  In this mode, all data is forwarded to the IP stack and transmitted.

- Unsolicited Results Code

Syntax	Description
+<cmd>:... **….**	Unsolicited result codes signal an event not directly associated with the latest issued AT command.

2.1.2 Process AT Command Response

Depending on the command and its results, the responses can be as follows:

Syntax	Description
`<CR><LF><result code><CR><LF>`	Verbose response to a command (after ATV1)
`[+<cmd>: ]free text<CR><LF>` `<CR><LF><result code><CR><LF>`	Verbose response to a command (after ATV1)
`CONNECT`	Response to particular commands
`>`	Prompt for data. Response to particular commands.

The <result code> mentioned in the table above can be:

Syntax	Description
OK	Command execution succeeded
NO CARRIER	Network communication lost
ERROR	Generic error. Can be replaced by the next two items.
+CME ERROR: <err>	Error related to MT operation
+CMS ERROR: <err>	Error related to the mobile equipment or thenetwork

2.1.3 Process Unsolicited Result Code

The DTE should monitor the URCs (Unsolicited Result Code) which may be issued at any time by the DCE and handle them.

Most of the time, no URC is inserted between the emission of an AT command and the reception of the result code thereof. However, this is not guaranteed by design. In this case the sequence could be:

- The host starts sending AT command AT+SQNSD=…
- The modem starts sending URC
- The modem completes URC transmission before echoing AT+SQNSD=… command
- The modem processes the AT+SQNSD=… command and replies OK; meanwhile, no other URC can be sent to the host.

It is good practice that the DTE pauses briefly (for example, 20 ms) after the reception of an AT command result code or URC before issuing a new AT command. This gives the module the opportunity to transmit buffered URCs and reduce the likelihood of the aforementioned situation.

2.2 Connection Manager

The connection manager is part of the application software running on the MCU. It enables and disables and manages the connectivity and, more generally the status of the product.

The connection manager’s task is to ensure that the connectivity is set up and restored in case of an unexpected situation:

- Long device activation delays
- Loss of network connectivity
- Communication loss between host and module

The connectivity manager development is the customer’s responsibility. Renesas provides generic rules and block diagram examples. The implementation is left to the customer.

2.2.1 Operator Modes

Several operator modes are predefined in the software. Entering an operator mode tunes the module the requirements of a specific network/ carrier:

- Supported RF bands to scan
- Predefined scanning profile
- Roaming enabled or not
  - When roaming is disabled, the modem does not attach with CEREG: 5, only CEREG: 1 is supported
- Feature group in UE capability
- PDN configuration
- LwM2M support

The operator mode can be selected with the AT+SQNCTM command. For products using MVNO SIM cards and operating on several networks, it is recommended to keep the operator mode set to standard mode. Other operator modes are reserved for products targeting a specific operator, using the operator’s SIM card, and requiring the operator’s certification. The settings of each operator mode are listed in the specifications of each operator the module is certified for.

The predefined operator modes are listed in the following table:

Operator/Bands	Roaming	UE capability	PDN configuration	LwM2M support	Handover activation
AT&T: 2, 4, 12	Enabled	MAC RAI disabled Banishment on failure enabled with the following parameters: Minimum number of connection establishment failures needed to evaluate the banishment (number T300 expiries): 5 Minimum duration required since the 1st failure before evaluating the banishment: 1 min Duration of banishment time: 6 min	PDN1 APN: broadband PDN2 APN: lwaactivate PDN3 APN: custom PDN4 APN: attm2mglobal Default Internet PDN: PDN1	Enabled	Enabled (Inter- and intra-frequency handovers)
On AT&T network, the APN provisioned for PDN1 is the one specified in AT&T requirements. However, it sounds like this PDN setting is rejected from the AT&T network with some AT&T SIM cards. In that case, the APN should be left blank for PDN1 with `AT+CGDCONT=1,"IPV4V6",""` .					
AT&T (roaming): 1, 2, 3, 4, 5, 8, 12, 19, 20, 28	Enabled	MAC RAI disabled Banishment on failure enabled with the following parameters: Minimum number of connection establishment failures needed to evaluate the banishment (number T300 expiries): 5 Minimum duration required since the first failure before evaluating the banishment: 1 min Duration of banishment time: 6 min	PDN1 APN: broadband PDN2 APN: lwaactivate PDN3 APN: custom PDN4 APN: attm2mglobal Default Internet PDN: PDN1	Enabled	Enabled (Inter- and intra-frequency handovers)
Docomo:1, 19	Disabled	Banishment on failure enabled with thefollowing parameters: Minimum number of connection establishment failures needed to evaluate the banishment (number T300 expiries): 5 Minimum duration required since the 1st failure before evaluating the banishment: 1 min Duration of banishment time: 6 min eDRX is enabled by default with a cyclelength of 81.92s and a paging time window of 5.12s	Default: Internet PDN: PDN1	Disabled	Intra-frequency handover is allowed. Inter-frequency handover is disabled.

Operator/Bands	Roaming	UE capability	PDN configuration	LwM2M support	Handover activation
Users planning to use AT&T in roaming mode must use default AT&T `SQNCTM` mode and add extra bands via `AT+SQNBANDSEL` (this is the only case where `AT+SQNBANDSEL` can be used to add bands). The bands selected depend on the target deployment region. Users may disable LWM2M or not depending on their own commercial agreement with AT&T with `AT+SQNDMCFG` command.					
KDDI:18, 26	Enabled	eDRX is enabled by default with a cyclelength of 10.24s and a paging time window of 1.28s	Default Internet PDN: PDN1	Disabled	Intra-frequency handover is allowed. Inter-frequency handover is disabled
Standard: 1, 2, 3, 4, 5, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 66	Enabled	Banishment on failure enabled with thefollowing parameters: Minimum number of connection establishment failures needed to evaluate the banishment (number T300 expiries): 13 Minimum duration in milliseconds required since the 1st failure before evaluating the banishment: 10 Duration of banishment time in seconds: 230	Default Internet PDN: PDN1	Disabled	Enabled (Inter- and intra-frequency handovers)
Verizon-no-roaming: 4, 13	Disabled	Banishment on failure enabled with the following parameters: Minimum number of connection establishment failures needed to evaluate the banishment (number T300 expiries): 13 Minimum duration in milliseconds required since the first failure before evaluating the banishment: 10 Duration of banishment time in seconds: 230	PDN2 APN: VZWADMIN PDN3 APN: VZWINTERNET PDN4 APN: VZWAPP PDN6 APN: VZWCLASS6 PDN7 APN: VZWCLASS7 Default Internet PDN: PDN3	Enabled	Enabled (Inter- and intra-frequency handovers)

Operator/Bands	Roaming	UE capability	PDN configuration	LwM2M support	Handover activation
Verizon: 4, 5, 12, 13, 17 ,20	Enabled	Banishment on failure enabled with the following parameters: Minimum number of connection establishment failures needed to evaluate the banishment (number T300 expiries): 13 Minimum duration in milliseconds required since the 1st failure before evaluating the banishment: 10 Duration of banishment time in seconds: 230	PDN2 APN: VZWADMIN PDN3 APN: VZWINTERNET PDN4 APN: VZWAPP PDN6 APN: VZWCLASS6 PDN7 APN: VZWCLASS7 Default Internet PDN: PDN3	Enabled	Enabled (Inter- and intra-frequency handovers)
T-mobile: 2, 4, 5, 12, 66	Enabled		PDN1 APN: iot.catm PDN2 APN: iot.catm.nc Default Internet PDN: PDN1	Disabled	Enabled (Inter- and intra-frequency handovers)

2.2.2 Network Connectivity

Network connectivity issues have several possible causes.

2.2.2.1 PLMN Selection

The principles of PLMN selection in E-UTRA are based on the 3GPP PLMN selection principles. First, the UE NAS layer selects a PLMN and the equivalent PLMNs as described in the figure that follows.

Then, the UE searches the configured E-UTRA frequency bands and, for each carrier frequency, detects the strongest cell. It reads the cell system information broadcast to identify its PLMN(s). The UE may connect to each carrier in turn (‘initial cell selection’) or use stored information to shorten the search (‘stored information cell selection’).

The UE searches for a cell :

- Whose PLMN is the selected PLMN, or an equivalent PLMN
- Which is not barred or reserved,
- Whose tracking area is not in the list of ‘forbidden tracking areas for roaming’ list.

If it cannot find a suitable cell, it looks to identify an acceptable cell whose attributes satisfy the cell selection criteria while not being barred. The UE then selects the PLMN to register on, according to the rules defined in the 3GPP specification 23.122.

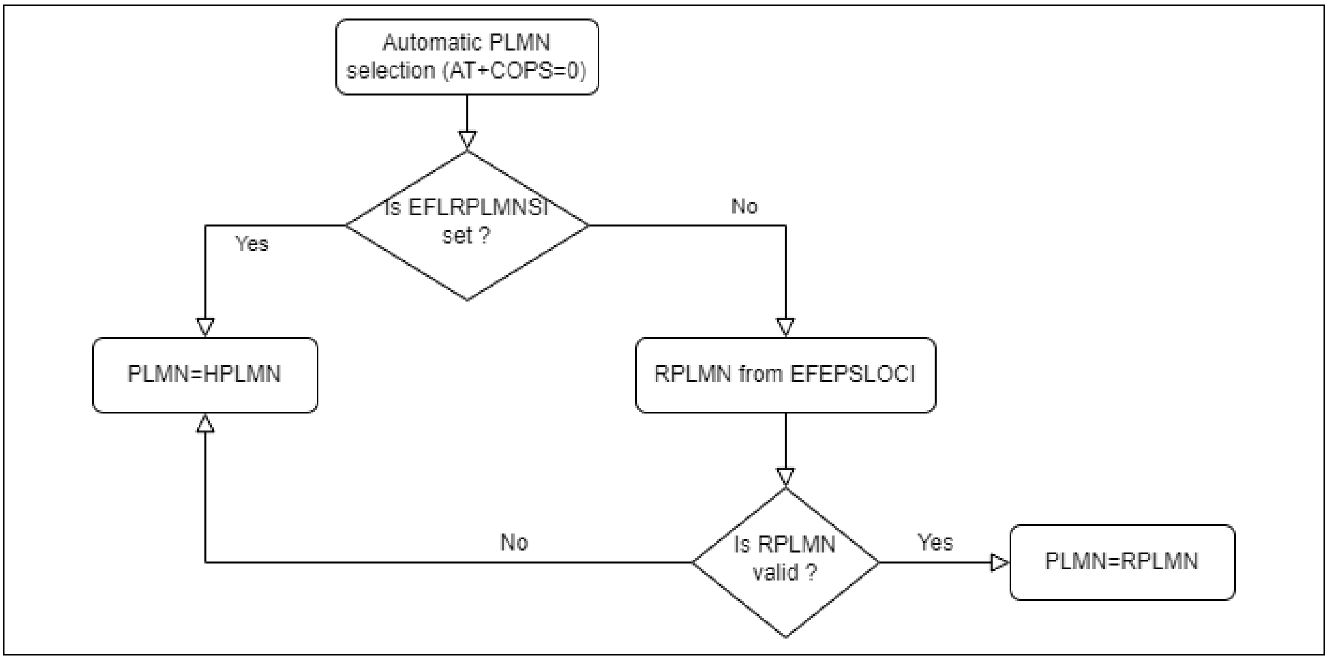


Figure 13. PLMN Selection

2.2.2.2 Scanning for Suitable Cells

While the modem scans for suitable cells, the network connectivity is down. The modem reports the scanning operation with the `+CEREG:2` URC. The host must wait for the `+CEREG: 1` URC. Scan time depends on the number of bands configured in the modem.

The scanning duration depends on the number of bands configured in the modem.

In standard operator mode, the modem scans all the 17 bands that it supports. The host can narrow down the number of bands to be scanned using `AT+SQNBANDSEL or AT+SQNCTM` commands. Some EARFCN are pre-configured in standard mode and are scanned first: 6200, 6300, 6400, 3700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890, 2500, 2600, 1350, 5900, 8750. The host MCU can modify the list of preferred EARFCN values with `AT+SQNEARFCNSEL`. See the *Use Cases with AT commands* document for more details. This scanning configuration persists at reboot.

- Cell detection duration per candidate EARFCN is 30 ms. Scanning the full 17 bands will take 186 seconds (~ 3 min).
- Once scanning is over, PLMN acquisition (decoding MIB and SIB1) for each candidate cell will take $2 \times 2 \times 80 = 320$ ms per candidate cell.

RYZ024 modules draw 75 mA at 3.8 V. The bands to be configured depend on the operator targeted for the device. Here are the bands that are the most frequently used for each region of the world:

Region	Bands
North America	2, 4, 5, 12, 13, 25
EMEA	1, 3, 8, 20, 28
Japan	1, 3, 8, 18, 19, 26
Australia	1, 3, 8, 28

If no suitable cells are found, the modem continues scanning the bands several times, with pauses in between each scan.

Note: There is no possibility to change the band priority.
For example, in standard operator mode, when all 17 bands are configured, the scanning goes as follows:

1. The modem first scans the two most recent valid frequencies on which it attached. If the MRU is empty(first boot), this step is skipped.
2. It then scans the list of pre-configured EARFCN.

3. Then the modem sweeps all the configured bands in four steps:
   A. First, for every configured band in the set {20, 8, 18, 25, 71}, it scans all EARCFN values ending in 0 or 5.
   B. Next, for every configured band in the set {28, 19, 13, 66}, it scans all EARCFN values ending in 0 or 5.
   C. Then, for every configured band {17, 1, 26, 3}, it scans all EARCFN values ending in 0 or 5..
   D. Finally, for every configured band in the set {2, 12, 4, 5}, it scans all EARCFN values ending in 0 or 5.
4. The modem sends a first `+CEREG: 4` URC if no suitable cell is found
5. The modem scans the list of pre-configured EARFCN again.
6. It then scans all configured bands in four steps:
   A. First, for every configured band in the set {20, 8, 18, 25, 71}, it scans all EARFCN not endingin 0 or 5.
   B. Next, for every configured band in the set {28, 19, 13, 66}, all EARFCN not ending in 0 or 5.
   C. Then, for every configured band in the set {17, 1, 26, 3}, all EARFCN not ending in 0 or 5.
   D. Finally, for every configured band in the set {2, 12, 4, 5}, all EARFCN not ending in 0 or 5.
7. For each band scan group, UE does the following operations in this successive order until it finds the requested PLMN:
   A. Carrier Detect: detect synchronization signals on each EARFCN. If all bands are configured, this operation takes:
      35 s for B20, 8, 18, 25, 71
      31 s for B28, 19, 13, 66
      35 s for B17, 1, 26, 3
      28 s for B2, 12, 4, 5
   B. Cell Detect/Cell Identify: decode MIB and SIB1 messages for each EARFCN from step 1.This step takes 300 ms per EARFCN if successful, and up to 1.9 s in case of false EARFCN detection).
   C. Cell Select: PLMN acquisition. This step takes around 200 ms for each cell detected in step 2.
   D. The scanning algorithm ends each time the PLMN detected corresponds to that requested. It is restarted if the UE gets rejected during the attach procedure, for example.
8. If steps 1, 2, 3, 4 and 5 above took less than 240 seconds, the modem starts again and does not send another `+CEREG: 4` URC after step 3d.
9. Finally, the modem first sends a second `+CEREG: 4` URC and repeats the steps 1, 2, 5a, waits 90 seconds, then steps 1, 2, 5b, waits 90 seconds, then step 1, 2, 5c, waits 90 seconds and lastly steps 1, 2 and 5d, waits 90 seconds.
10. The modem repeats step 9 indefinitely.

2.2.2.3 Out of Coverage

LTE-M coverage info is available here.

If the UE is in a location where no Cat M1 network is available, the modem will send `+CEREG: 4` notifications at the end of the step 3d of the scanning procedure described above. This `+CEREG: 4` URC will be followed by a `+CEREG:2` to indicate that the modem continues looking for a suitable cell. The host can either power off the module for 24 hours or change the bands configured for scanning.

The MCU defines the bands to be scanned with `AT+SQNBANDSEL` command and reconfigures the modem when no coverage is found after a given period.

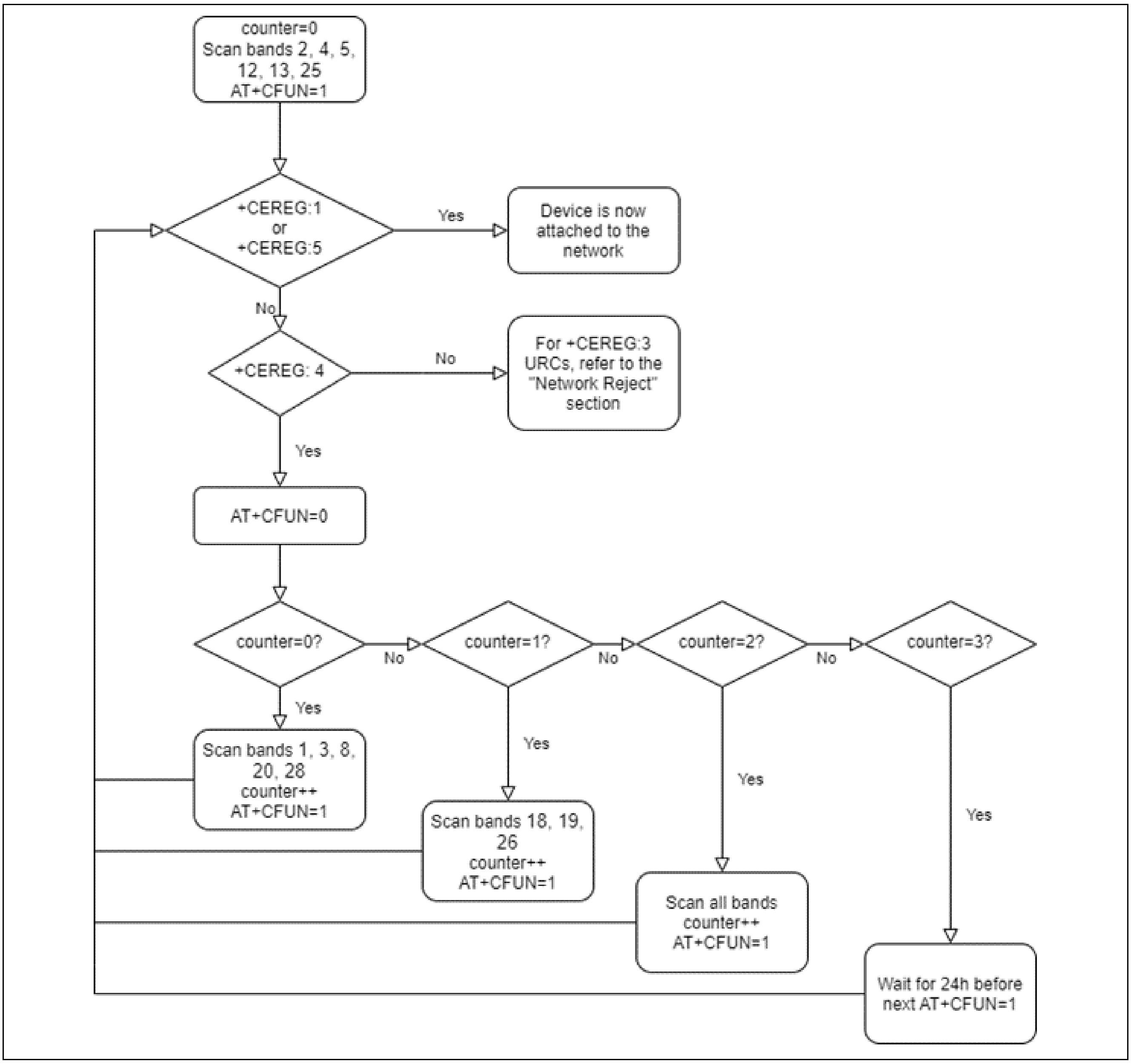
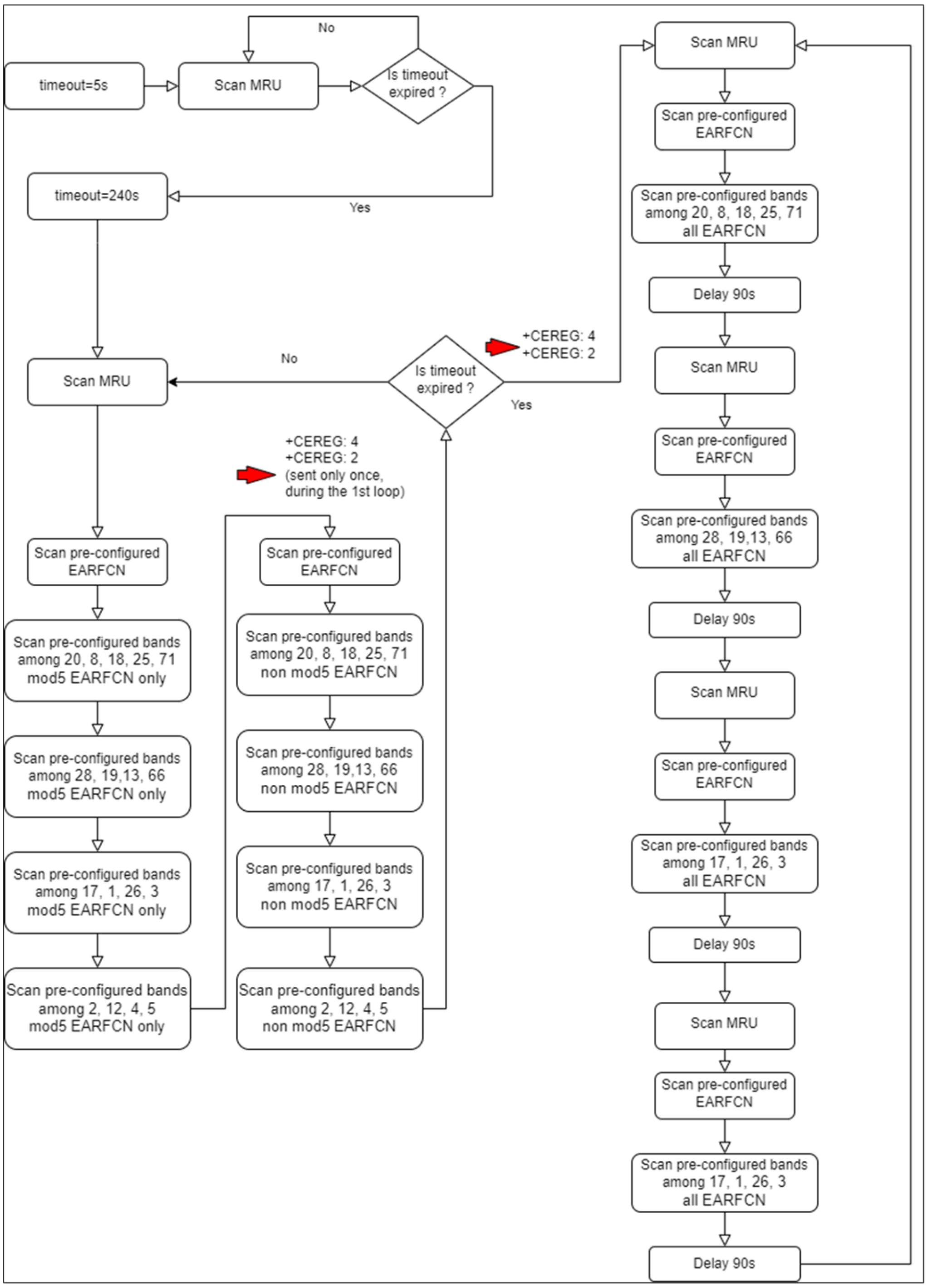


Figure 14. Example Flow

2.2.2.4 Network Reject

The network can reject the modem if it is not configured with the correct APN or its IMEI is not valid from the network point of view.



The host application should activate the +CEREG URC using AT+CEREG=3 before sending AT+CFUN=1to get the <reject_cause>. It is also possible to ask for a reject message once the +CEREG URC is received by sending AT+CEER.

The +CEREG URC indicating the reject cause is followed by the +CEREG: 2 URC, indicating that the UE keeps searching for another suitable cell. Note that in some cases, described in 3GPP standard, the modem can send a +CEREG: 0 URC when getting rejected by the network. The modem may even start a timer during which the LTE stack is forbidden from reattaching to the network. In that case, it is recommended to switch off the device and retry later.

The most common reject causes are the following:

- No Suitable Cells in Tracking Area
- Illegal mobile equipment
- IMSI unknown at HLR
- PLMN not allowed
- Location area not allowed
- Roaming not allowed in this location area
- Network failure
- Network congestion

Moving the device to another location may help.

If the registration type is manual (`+COPS = 1`), then the host must restart a manual PLMN search or force automatic PLMN selection mode (`AT+COPS=0`).

If the registration type is automatic (`+COPS = 0`), the modem may look for an allowed PLMN if the rejection cause was roaming restriction.

An illegal mobile equipment error indicates possible problems with either the SIM card or the modem's IMEI.

2.2.2.5 Coverage Loss

Once the UE is attached to the network, it goes into RRC connected mode. In poor radio conditions, the UE radio link failures are likely. `+CEREG` URCs, such as `+CEREG: 80` and `+CEREG:4`, warn the MCU of the radio link failure. It is also possible to activate `+SQNDRDY` URCs. These URCs are sent before the `+CEREG` URCs and can be useful in case of temporary loss of coverage.

2.2.2.6 RRC Connection Release

If the UE is attached to the network but inactive (no data exchanged with the network), the network releases the connection after the expiration of the inactivity timer. The value of this inactivity timer is carrier dependent and is not shared with the modem. It usually varies between 5 and 30 seconds. Following is a graph extracted from the 3GPP standard, explaining the RRC connection release mechanism:

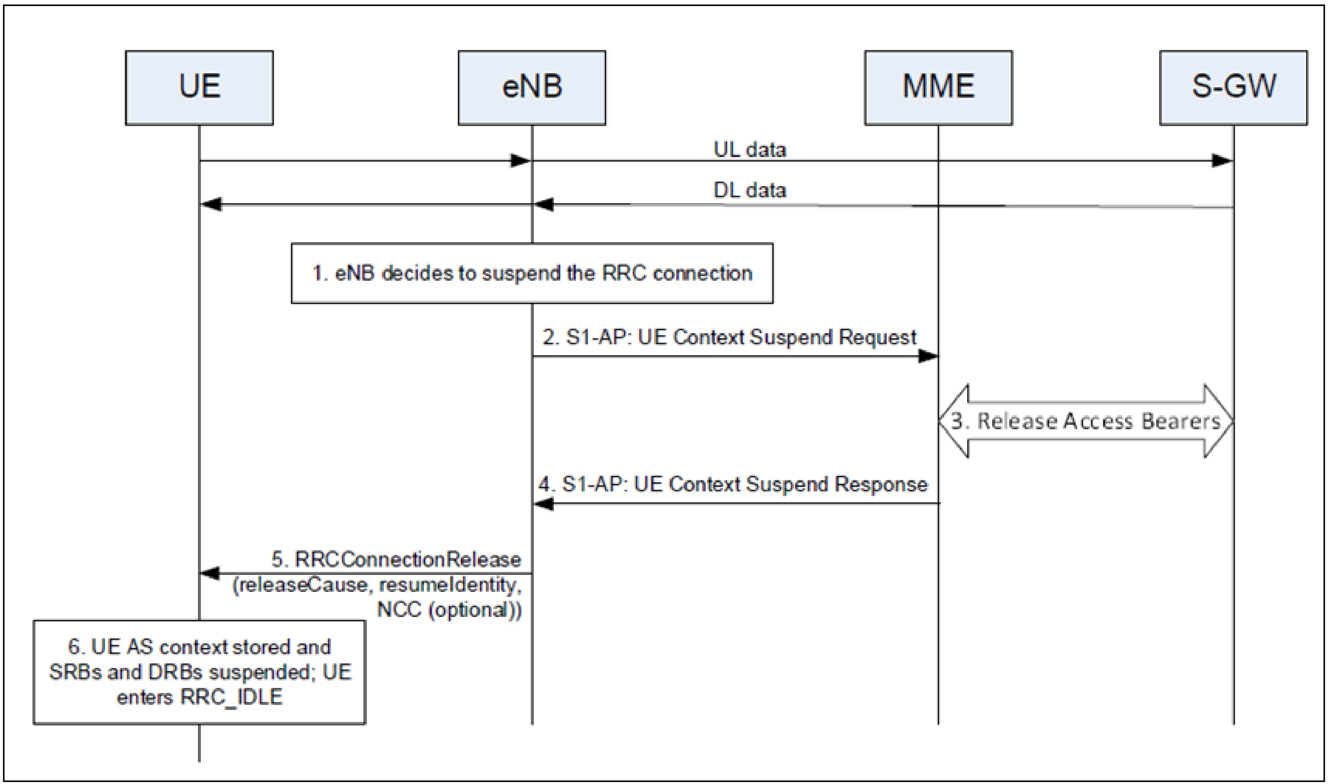


Figure 15. RRC Connection Release Mechanism

If, for some reason, the UE misses the RRC connection release message, it keeps listening to the network and does not enter power saving modes. Therefore, UE data inactivity monitoring feature has been introduced by 3GPP, allowing UE to release RRC connection if no data activity is detected by UE after a duration called "`dataInactivityTimer`" (timer value sent by eNodeB). In case this feature is not supported by the network (no "`datainactivityTimer`" sent by eNodeb), it can be activated on the UE side in a self-implementation mode using the `AT+SQNDIT` command: the UE monitors data inactivity on its side as well and quits listening to the network after 120 s of data inactivity. This data inactivity timer value can be tweaked with the `AT+SQNDIT` command. This timer must never be shorter than three times the network inactivity timer. Please contact you operator to obtain the inactivity timer value of its network.

2.2.2.7 SIM

(1) Multi IMSI SIM Support

Some SIM cards, especially MVNO SIM cards, implement a multi IMSI feature. They behave as follows:

- They have a default IMSI used until the network's MCC is known
- Once the modem is attached and the MCC is known, the SIM switches from default to primary IMSI if it exists
- If the primary IMSI reports limited service after a specific timer expires, the SIM falls back on the default IMSI
- In the worst case scenario, therefore, an out-of-the-box attach in the field can take three full scans:
  - First attach with default IMSI
  - Second scan with the primary IMSI, which fails to attach
  - Third scan with default IMSI that succeeds

(2) SIM Activation – Verizon Specific

The first time a non-activated Verizon SIM card is inserted into a CAT M1 device, the SIM launches a BIP session for its activation.

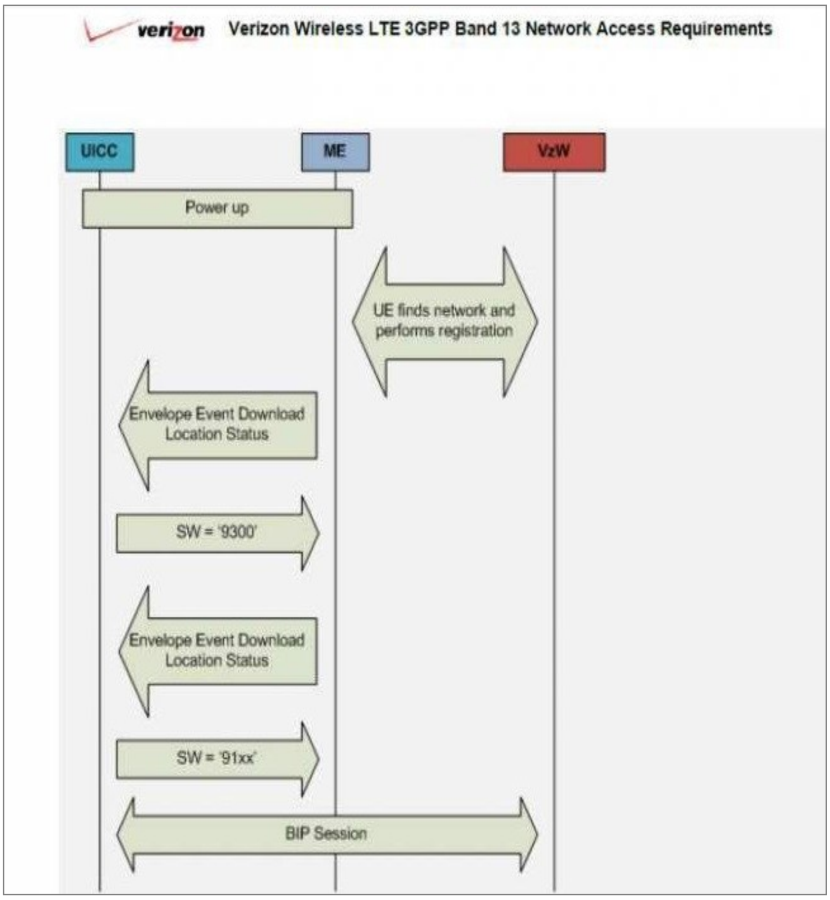


Figure 16. Verizon-specific SIM Activation

In this case, although there is no data connectivity for a short while, the MCU must not reset the modem. The delay varies according to the SIM, the network and the RF conditions. It can take up to a few minutes.

There is no specific URC notifying of an ongoing BIP session. However, it is possible to activate the SIM status `+SQNSIMST` URCs. These URC are disabled by default and can be turned on with `AT+SQNSIMST=1`. The host receives a URC when the SIM card is ready.

2.2.3 Network Connectivity Loss

If case the modem managed to connect to the network, there are multiple reasons why the network connectivity could be lost over time:

- RF conditions: The propagation channel can change and lead to radio link failures, whether the device is moving or static. The connection manager is informed about connectivity loss by a `+CEREG 0` or `4` URC. These URC can be activated/deactivated with the `AT+CEREG` command.
  - Please refer to Monarch AT commands reference manual and 3GPP TS 27.007 section 10.1.22 for more details on the `+CEREG` command.
  - The modem can also emit the proprietary URC `+CEREG:80` when PLMN is lost.This URC is sent as soon as the network connectivity is lost. It will be then followed by a `+CEREG: 1` URC if the modem can attach to the network again or by a `+CEREG: 2` URC while the modem scans for suitable cells.
- Network reject
  - The network can reject the modem after a cell reselection.
  - The host application should activate the `+CEREG` URC with `AT+CEREG=3` to get the <reject_cause>.
- Unidentified reason
  - This is a blanket cause for all possible software bugs that were not identified during the product certification and field tests.
  - The connection manager must manage that scenario to make sure that the connectivity can be recovered.
- Modem FOTA
  - Connectivity is lost during modem upgrade (reboot of the modem).
  - During the downtime, the connection manager must not reset the modem and must wait for the completion of the upgrade.
  - Refer to section 3.2, Firmware Upgrade Over-the-Air to get the list of URCs sent during firmware upgrade.

2.2.4 AT Communication Interruption

AT commands are the only way for the MCU to communicate with the modem. Several reasons can cause the modem to be unresponsive to AT commands.

2.2.4.1 AT Commands Timeout

The application software can trigger a modem reset if it receives no answer to an AT command. The current *AT commands reference manual* specifies no timeout for synchronous AT commands.

This is because many commands depend on the network. The host should reset the module after 60 seconds of no response, barring some specific data AT commands which can take longer to execute on very slow networks.

2.2.4.2 Software Upgrade

During a modem software upgrade, local or OTA, the modem disconnect from both the network and the host. The connection manager must not reset the modem during a firmware upgrade.

2.2.4.3 Data Mode

Before most IP data transfers, the modem enters data mode and accepts data from MCU. In this mode, no AT response is possible. Please refer to *AT Commands User Manual* for more details on the data mode.

A typical example is the use of `AT+SQNSSENDEXT` to send data to the server using a socket. The second parameter of this command contains the length of the data to be sent. If the data block sent by the MCU is shorter than the length specified in the command, the modem stalls and keeps the UART in data mode. This usually happens when the length given in the command takes the termination characters (for example, '\r\n') into account, but the data does not include them.

2.2.4.4 PPP Session

The modem supports the PPP protocol for data transfer on top of data over AT commands. In that case as well, the host MCU will first have to pause the PPP session to enter AT command mode again.

2.2.5 Data Retries

The device is required to follow the TS35 rules defined by GSMA about data retries to avoid flooding the network.

The following scenarios are tested during device certification:

Test case Id	Test case name
TS35_5.1_TC_001	Basic RRC and data connection establishment /release, ensuring connection requests are not flooding
TS35_5.1_TC_008d	Failure scenario (wrong APN)
TS35_5.1_TC_008g	Failure scenario (IoT server not reachable)
TS35_5.1_TC_008h	Failure scenario (SMSC not reachable)

TC 001 checks that the IoT Device Application is capable of sending data frequently; there is no specific requirement at the connection manager level. The other three test cases check the IoT Device Application's behavior whenever the network communication requests fail.

The connection manager must not initiate more than thirty retries in one hour (test duration) to pass. The simplest way to comply is setting a suitable back-off period after each failure. For example, following a failure to setup a data connection, the MCU should wait five seconds before retrying. If the new attempt also fails, the MCU should wait twenty seconds before trying again, and so forth.

To pass the SMS transfer (TC_008h) test, the host application must not retry sending the SMS more than eight times. This module automatically resend every unsuccessful SMS three times.

Each operator has its own data retry requirements, if any. Generally speaking, the connection manager should avoid piling up retries as far as possible.

2.2.6 Power Management

2.2.6.1 Protocol Level

(1) Power Saving Modes

For power consumption sensitive products, low power management is mandatory. Besides the legacy RRC IDLE mode, RYZ024 modules also support eDRX and PSM modes which comply with the 3GPP standard.

During PSM-Idle or eDRX-Idle duration, the modem cannot be reached from the network.

RRC Idle, PSM or eDRX modes should be chosen according to the expected inactivity period of the product:

- Products which must always be reachable must use the RRC Idle mode. They must not be power consumption sensitive.
- Products which must be reached every few seconds up to every ~44 minutes (in LTE- M), can use eDRX mode. NB-IoT eDRX supports a longer sleeping time with respect to LTE-M. Please refer to 3GPP standard for the details.

Caution: A device in eDRX mode must perform TAU procedures. The timer T3412 is set by the network and cannot be negotiated. These TAU procedures must be accounted for when estimating the product's power budget.

- For products which are active every hour to every few days, PSM mode can be used.
  - PSM efficiency highly depends on the network settings. Some networks do not accept large values for T3412-extended, which results in unwanted TAU procedures draining the battery. Sometimes the network does not allow very small values for T3324, which causes the device to remain in RRC Idle mode before entering Deep Sleep mode.
- If power consumption is critical, the connection manager can turn off the modem using `AT+CFUN=0 or 4` instead of relying on one of the aforementioned modes. The network operator must agree with this policy best fitted for devices talking no more than once or twice a day.

The connection manager must be aware that the network is not obliged to support PSM or eDRX modes. If power consumption is an issue, the connection manager must ensure that the device does not remain in RRC Idle mode all the time.

Please refer to the *Use Cases with AT commands* and the *Power Consumption Measurement* application notes for more details on how to set the PSM and eDRX modes.

Mode	Wake-up latency
Deep sleep	< 2 secs
Sleep	< 15 ms
Standby	< 1 ms
Modem active	< 1 ms

(2) PDN Idle Timer

The network sets a PDN idle timer whose value is unknown to the module. When the PDN idle timer expires, the network disconnects the modem from the network.

In PSM mode, if the PDN idle timer is lower than the T3412 value, the modem can find itself disconnected when it wakes up. It must therefore perform a full reattachment procedure, losing the benefits of the seamless reconnection.

In eDRX, the PDN idle timer can expire during the eDRX idle period. In such a case, the UE becomes unreachable until it performs a mobile originated activity.

Each carrier is free to set its own PDN idle timer value, or to offer private APNs with custom PDN idle timer values. The customer should contact their SIM provider and make sure that the PDN idle timer value is compatible with its application.

(3) Sockets

Data sockets settings are unaffected by Sleep and Deep Sleep modes: when waking up from Sleep or Deep Sleep mode, the MCU does not need to re-establish the socket connection. The socket is kept open on the UE side even if the platform enters Deep Sleep mode. The socket can however be closed by the remote server because of inactivity. If the socket is closed while the UE is in Sleep or Deep Sleep mode, it will not be notified. The socket state returned with the `AT+SQNSS` remains unchanged. An error occurs when the MCU attempts to send data.

If the connection is secured, the modem automatically reestablishes it when waking up from Sleep or Deep Sleep modes. The TLS, or DTLS, handshake strains the system during the handshake phase, requiring multiple exchanges with the server and many CPU cycles to compute the keys. This results in long data link establishment and high power consumption, as the modem is fully active and connected to the network during this phase. To improve the handshake's performance, TLS/DTLS specifications introduced a session restoration feature that allows a client to pick up an earlier established session state. The server may elect not to exchange cookies at session's reestablishment.

This feature can be activated with the `AT+SQNSPCFG` command.

(4) Relaxed Monitoring

Depending on the RF signal strength and the network settings, the UE is required to monitor the neighboring cells' RSRP and RSRQ. When the UE is in eDRX Idle and needs to perform measurements on the neighboring cells, it wakes several seconds before going back to eDRX Sleep, increasing its power consumption. The RF surroundings of a static device are not likely to change significantly over time, except if the network topology is updated or the device's environment evolves. In such conditions, the 3GPP standard allows the device to drastically reduce the number of neighbor cells' scans to save power, enforcing a minimum of only one measurement per day, in order to detect infrequent RF environment changes. This is a real gain in terms of power consumption for static devices located on cell edges.

Relaxed monitoring feature helps reduce power consumption when the serving cell signal remains good and stable.

When relaxed monitoring is on, cell reselection rate is greatly reduced. The device scans for a better cell only if the RSRP value exceeds a given threshold. When a device reconnects to the network after a DRX sleep state, it may not use the best cell for transmission. To improve data reception's reliability after a transition from DRX sleep to connected mode, the modem should perform a cell reselection when resuming the RRC connected mode. This step can be skipped if the last cell reselection session is deemed recent enough.

In addition to 3GPP specification requirements, the platform should perform an additional check on the CINR value, as Renesas considers that the RSRP alone does not fully qualify the RF signal quality. Interfering users can degrade the CINR while the RSRP stays constant. Thus, if the current cell's CINR drops below a given threshold, then UE should scan the neighbor cells.

Relaxed monitoring can be activated with the `AT+SQNRMON` command.

Measurements are performed when one of these conditions is met:

- The current cell's RSRP is out of the acceptable range defined by the 3GPP relax monitoring feature.
- The current cell's CINR is out of the acceptable range. The threshold value is set by the `<cinr_thold>` parameter of the `AT+SQNRMON` command. Default value is -90 dB.

This relaxed monitoring feature can be privately enabled if the network does not support it. In this case,the UE needs to define its own RSRP criterion and maximum delay between two cell reselections, using the `<rsrp_hyst>` and `<resel_before_tx_timer>` parameters of the `AT+SQNRMON` command. This device initiated relaxed monitoring feature is not 3GPP compliant and the operator must authorize its use. Device initiated relaxed monitoring use is the device owner's responsibility. It can be enabled using the `<device>` parameter of the `AT+SQNRMON` command.

The modem respects the following activation rules:

- The modem uses the configuration set by users with the `AT+SQNRMON` command.
- If none is set, the network advertised configuration is used.
- If the network does not support relaxed monitoring, the modem uses the default firmware configuration;
- Device initiated relaxed monitoring feature is deactivated by default.

(5) Handover Configuration

If the device is static or connected to the network during very short periods of time, the handover mechanism may add extra activity and lead to higher power consumption for little profit. In that case, it is recommended to disable handover support with `AT+SQNHOCFG`. Note that this handover support can only be changed for the standard operator mode.

(6) LwM2M

RYZ024 modules have a LwM2M stack, since it is required to pass certification on specific networks. LwM2M stack operation impacts the power consumption. First, it creates a second PDN that requires exchanging messages with the network. The LwM2M client also starts a bootstrap exchange with the server. If it fails, the client retries it periodically. This can either prevent the module from entering low power modes or wake it up. It is possible to deactivate the LwM2M client with `AT+SQNDMCFG`. This should be done in agreement with the operator.

2.2.6.2 Platform Level

The host MCU must handle the wake sources (RTS0,RST1, and Wake0) and drive them high when the module should enter Sleep mode. Even if all wake sources are disabled, the module does not enter Sleep or Deep Sleep mode if:

- The device talks to the network
- URCs or data are pending in the UART buffer

To avoid having URCs pending in the UART buffer, all UART that are not connected to a MCU should be defined as debug UARTs (here, UART1):

```
AT+CFUN=5

AT+SQNHWCFG="uart1","enable","rtscts","921600","8","none","1","dcp
"AT^RESET
```

When there is no network nor UART activity, the platform enters power saving modes. Use AT+SQNIPSCFG to configure how long the platform waits before entering low power modes after the last character is sent over the UART. As long as the UART inactivity timer has not run out, the module does not enter low power mode. Once the UART inactivity time has elapsed, the module can enter low power if all the other necessary conditions are met.

The authorized wake-up latency is the maximum time the module can take to resume operational mode when the host MCU needs access to the modem's services again. Resuming operational mode takes longer in 'Deep Sleep' mode than in normal 'Sleep' mode. The module always chooses the most efficient low power mode compatible with the preset wake-up latency. A latency shorter than two seconds typically prevents the module from entering 'Deep Sleep' mode. The default value for the wake-up latency is five seconds and can be altered with the AT+SQNPSCFG command.

The RING line toggles when URC or data are received. The ringing time defaults to five seconds. This value can be modified using the AT+SQNRICFG command. The modem platform remains active when the RING line is active. The same AT command also allows for any combination of URC and data as the triggering source, or for disabling the RING line altogether.

The modem sends no URC when exiting Sleep or Deep Sleep modes. The host MCU should monitor the CTS line if hardware flow control is activated to detect that the modem is ready to receive AT commands. If hardware flow control is disabled, the PS_STATUS line goes up as soon as the platform is out of Sleep or Deep Sleep mode. The MCU should then send "AT+CFUN?" and wait for the "OK" response to make sure that the UARTs are operational, as explained in section 1.2.3, Wake source.

Renesas provides several AT commands and URCs returning statistical figures to monitor the power consumption and predict the lifetime of a product on battery:

- Counting the +SYSTART URCs gives the number of reboots
- The 1V8 power supply and the PS_STATUS line indicate the time spent in Sleep and Deep Sleep modes
- The number of wakes from LPM can be obtained by monitoring the wake-ups triggered by the MCU
- The AT+SQNRXTXSTATS command displays the time spent in Rx and Tx modes. The Tx time is sorted according to the output power. The granularity is finer for high output powers since the PA's contribution increases with output power.

With all the above inputs, the customer can build a model to estimate power consumption. Training data are collected during field measurements of the product's power consumption, while sampling the relevant inputs as well. The data is then fed into a model that predicts the power consumption under various conditions.

2.2.7 Examples of Implementation

The following section provides typical examples of connection manager implementations for devices in different low power modes.

2.2.7.1 PSM

The device is an environment air monitor waking up regularly depending on a timer (Timer3).

To save battery the device is configured in PSM mode with the following timers (assuming that the network accepts these values):

- T3412: 2 hours
- T3324: 16 seconds
- Timer 3 should be set so that T3324 < Timer3 < T3412

Here is the typical use case:

- The device is registered to the network, goes to RRC Idle, and enters PSM after T3324 fires.
- Each time Timer3 expires, the modem is woken up:
  - If possible, the UE connects to the network, sends data, and then goes back into PSM for another period of Timer3.
  - If the modem cannot connect, the modem continues scanning for a period decided by the connection manager (Timer1).
    - If no cell is found, the modem is reset.
    - After three consecutive resets, the modem is shut down for a period defined by Timer2.

In this example, it is assumed that the MCU does not enter low power modes. If the MCU also supports low power modes, the RING line should be used to wake it up.

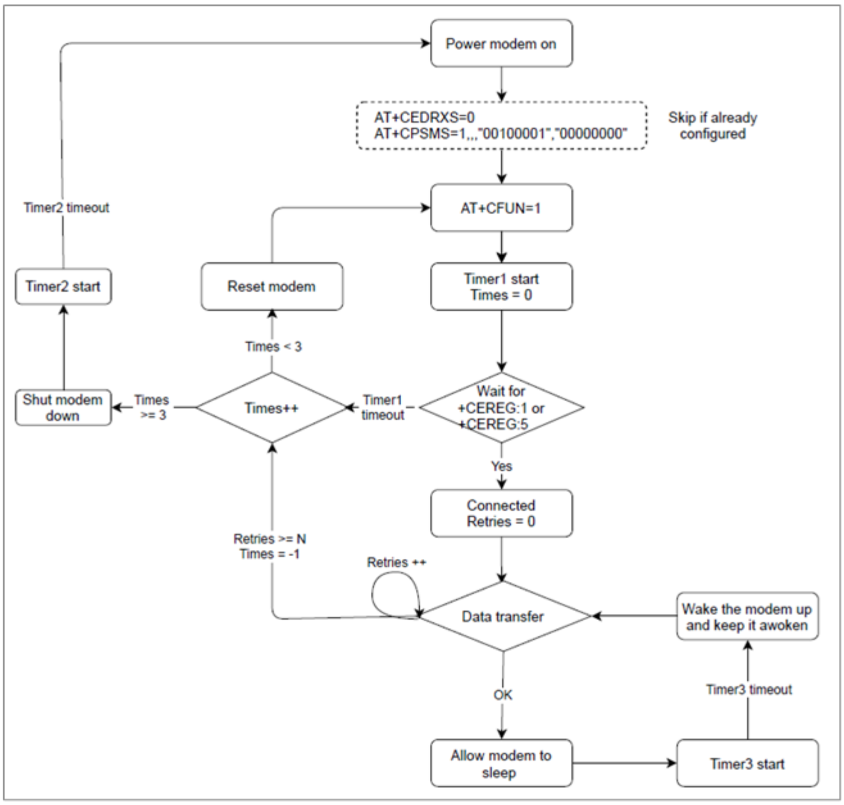


Figure 17. PSM Mode Example

The timers' values depend on the application and on the power consumption constraints of the device.

- When "Timer1" is started, the modem scans according to pre-defined parameters. To reduce power consumption, the scanning algorithm includes pauses. Please refer to section 2.2.2.1, PLMN Selection for the description of the scanning rules.
  - Typical recommended value of "Timer1" is several minutes: 5 minutes
  - Typical recommended value of "Timer2" is several hours, depending on the application
  - Timer3's value depends on how often data must be sent. Timer3 value should be greater than T3412-extended's value to avoid wasting energy in spurious TAU procedures.

The device should set the number of data transfer retries (N in the above diagram) according to the TS35 rules (see section 2.2.5, Data Retries for more details).

2.2.7.2 eDRX

The device is a tracker waking up regularly depending on a timer or motion. The tracker should also be reachable from the network within short period of times.

To save battery, the device is configured in eDRX mode with the following parameters (assuming network accepts that value):

- eDRX cycle: 327.68 seconds
- PTW: 5.12 seconds

Here is the typical use case:

- The device is registered to the network and enters eDRX after one data transfer
- At each eDRX cycle, the modem wakes up and monitors the paging opportunity for the duration of the PTW.
  - If there is network coverage,
    - The modem checks if there is a pending message (SMS in this example) and notifies the MCU using a URC. The MCU decides what to do.
    - If there is no pending message, the modem goes back to sleep for the next eDRX cycle.
  - If there is no network coverage anymore, the modem will continue scanning for a period of time set by the connection manager (Timer1).
    - If no cell is found, the modem is reset.
    - After three consecutive resets, the modem is shut down for a period of defined by Timer2.
- If the tracker is moving, the MCU may decide to send messages more frequently. In this case the MCU can wake the modem up and send data every time Timer3 expires.
- Note that in this example, it is assumed that the MCU does not enter low power modes. If the MCU also supports low power modes, the RING line should be used to wake it up.

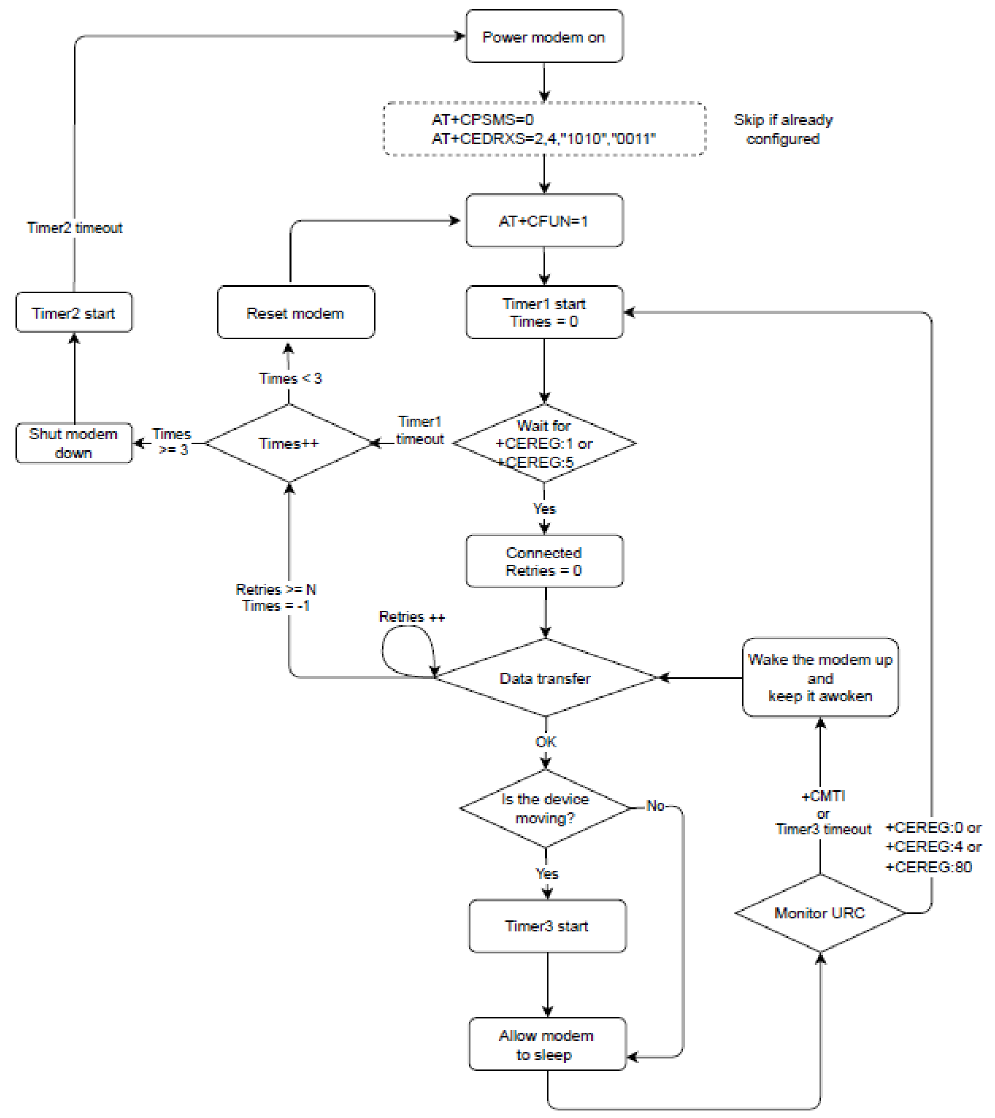


Figure 18. eDRX Mode Example

The timers' values depend on the application and on the power consumption constraints of the device.

- When Timer1 is started, the modem scans according to pre-defined parameters. To reduce power consumption, the scanning algorithm includes some pauses. See section 2.2.2.1, PLMN Selection for the description of the scanning rules.
- The recommended value of Timer1 is several minutes: 5 minutes
- The recommended value of Time 2 is several hours, depending on the application
- Timer3's value depends on how often the data must be sent when the device is in motion.

The device should set the number of data transfer retries (N in the above diagram) according to the TS35 rules (see section 2.2.4, AT Communication Interruption for more details).

2.2.7.3 CFUN0/CFUN4

The device is a push button, which only sends data.

Since the sleep period is higher than 6 hours, it uses `CFUN1/CFUN4` mode instead of PSM.

Energy efficiency demands the MCU issue `AT+CFUN=4` (or `AT+CFUN=0`) as soon as all data have been sent.

Here is the typical use case:

- The device is registered to network and sends data
  - When the data transfer is over, the MCU turns the modem off using `AT+CFUN=4` or `0`
- Each time Timer3 expires, the MCU powers on the modem again with `AT+CFUN=1`
  - If there is network coverage, the UE connects to the network, sends data and is shut down again by the MCU for another Timer3 duration.
  - If the network coverage is gone, the modem keeps scanning for a period of time set by the connection manager (Timer1).
    - If no cell is found, the modem is reset.
    - After three consecutive resets, the modem is shut down for a period defined by Time2.

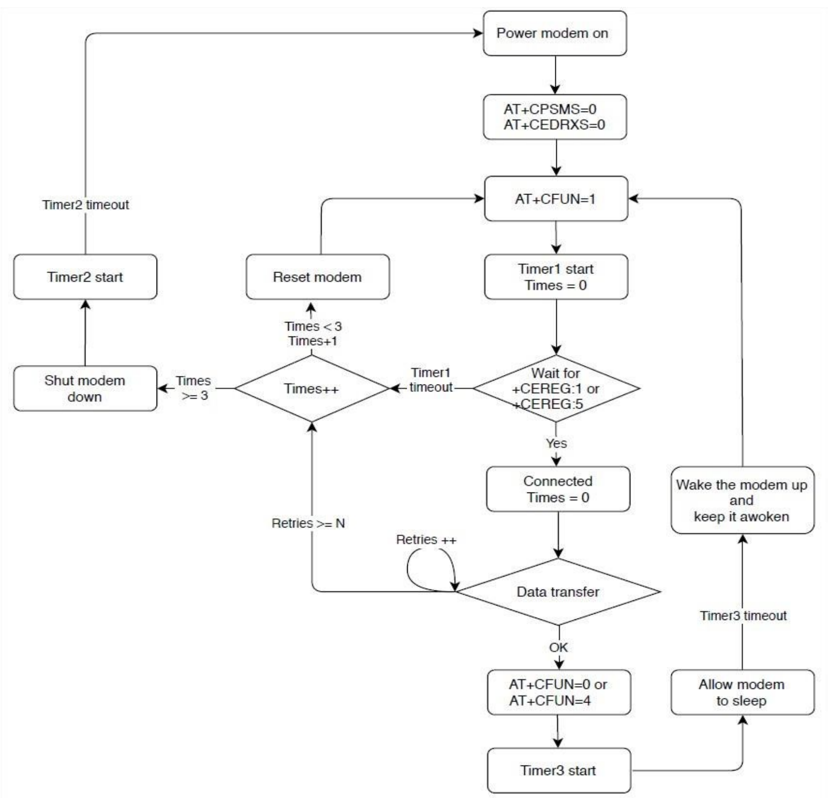


Figure 19. CFUN0/CFUN4 Use Case Example

The timers' values depend on the application and also on the power consumption constraints of the device.

- When Timer1 is started, the modem scans according to pre-defined parameters. To reduce power consumption, the scanning algorithm includes some pauses. See section 2.2.2.1, PLMN Selection for the description of the scanning rules.
  - The recommended value of Timer1 is several minutes: 5 minutes
  - The recommended value of Timer2 is several hours, depending on the application
  - Timer3's value depends on how often data must be sent.

The device should set the number of data transfer retries (N in the above diagram) according to the TS35 rules defined for data retries (see section 2.2.5, Data Retries for more details).

3. Firmware Update

During the product's lifetime, the firmware has to be updated, either locally or over-the-air.

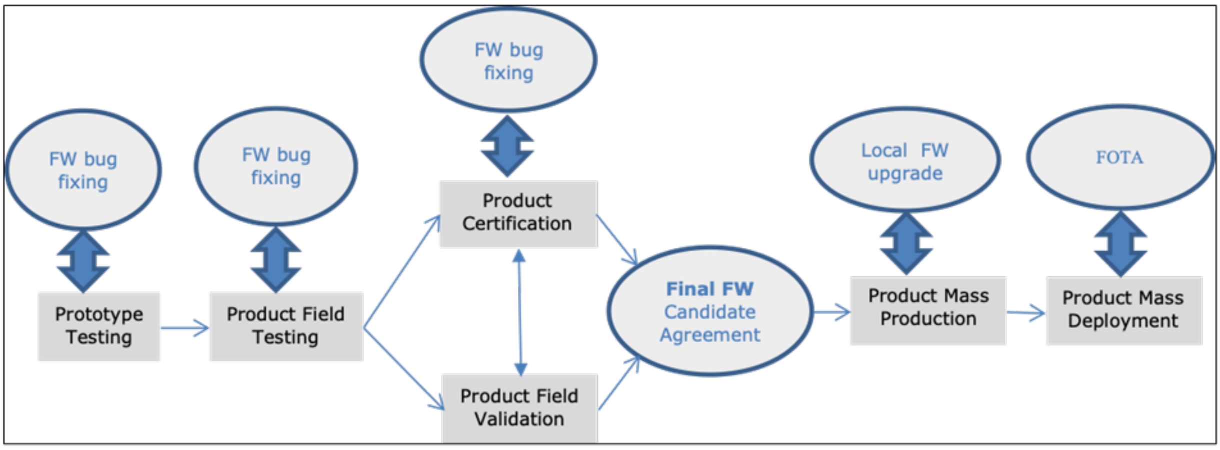


Figure 20. Firmware Update

3.1 Local Firmware Update

Renesas's Firmware Upgrade tool (SFU) performs local firmware upgrade. Please refer to the ***SW Upgrade Procedure*** application note for more details.

Compared to FOTA, local upgrade is more flexible (all parts of the software image can be updated) and faster. Furthermore, since it does not require any download from the network, and it does not impact the data plan.

The local upgrade is mostly used during the following phases of a project:

- Prototype testing
- Product field testing
- Product certification
- Product field validation
- Manufacturing

The firmware often needs to be updated during manufacturing, since the version shipped is not guaranteed to be up-to-date.

Once the product is widely deployed, the firmware must be updated using FOTA. If the product has multi-link radio capabilities, the firmware can be downloaded over WiFi or BLE, with no data plan cost, and then pushed from the MCU to the module. Please refer to the ***SW Upgrade Procedure*** application note for guidelines on how to implement such a tool.

3.2 Firmware Upgrade Over-the-Air

3.2.1 Differential Upgrade

RYZ024 based modules support differential software upgrade over the air. Full software upgrade is supported in local mode only.

Cat M1/Cat NB1 devices throughput is low and can fall even lower under poor RF conditions. Using a full firmware image could take a long time, typically several hours for a device located on a cell's edge, or even fail. If the device is battery powered, upgrade procedures can drain the battery very quickly. Additionally, IoT devices' data plans are often limited. Differential upgrade is therefore recommended.

Although differential and full upgrade lead to the same final product, differential upgrades need paying attention to a few points.

First, the differential upgrade is tailored to two specific versions of the software. Thus, unless the current software version matches the reference image used to generate the DUP file, the upgrade will fail.

The firmware image is made of four different parts:

- Boot ROM
- Updater
- UE firmware
- Filesystem

Any of these parts, except for the boot ROM, can be updated over the air, together or separately.

Upgrading the filesystem part will only impact Renesas' filesystem partition; the user filesystem partition will remain unchanged.

The differential image is built file by file, meaning that the following file operations in the differential filesystem image are supported:

- File add: the file exists in the target but not in the source
- File delete: the file exists in the source but not in the target
- Directory add: the directory exists in the target but not in the source
- Directory delete: the directory exists in the source but not in the target
- File diff: the file exists in both source and target, but the content differs

⚠ A directory delete erases all the files and subdirectories that the directory contained.

In most cases, the UE firmware is the only part of the module image actually upgraded once products are deployed.

The differential package between the last and the one before the last official software released by Renesas is available on Renesas cloud. Customers can also generate their own differential image if they need to upgrade from another software version.

3.2.2 Differential Image Generation

There are two ways to generate a differential package.

Differential packages are output by:

- A Python script delivered by Renesas
- Or using Renesas PXL SDK (opened to some specific customers).

Note: For the latter case, please refer to the PXL SDK User's.

The gain for differential upgrades in terms of payload size is significant, mainly for the updater and UE firmware parts.

3.2.2.1 Preparation

First get the following packages

`xxxxx_BIN_SQN34X0-GECKO_XXXX.tgz`

This package contains several *Python* tools, including the one needed for differential image generation

`RYZ024A_xxxxx.tgz` and `RYZ024A_yyyyy.tgz`

Both the current and the updated platform packages. These packages include the boot Rom configuration files.

You will need a *Unix*™ environment. We recommend using *Ubuntu* operating system 18.04 or 20.04.

Python 2.7 is mandatory for this differential image generation as well as a 64-bit distribution You can check the OS version with:

```
uname -a
```

Then make sure to install **python-dev** package as follows:

```
sudo apt-get install python-dev
sudo apt-get install python-pip
```

Install **lzma** dev library:

```
sudo apt-get install liblzma-dev
```

At last, install the following *Python* tools as well

```
pip install humanfriendly
pip install pyelftools

pip install backports.lzma
pip install bitstruct

pip install zstandard
```

3.2.2.2 Differential Image Generation

Following is a detailed example of differential image generation from release LR8.0.0.3-52128 to LR8.0.0.3-52148 for the RYZ024 module.

Here is the list of the needed packages:

- RYZ024A_LR8.0.0.3-52128.tgz

  The platform package of LR8.0.0.3-52128 software release

- RYZ024A_LR8.0.0.3-52148.tgz

  The platform package of LR8.0.0.3-52148 software release

- xxxxx_BIN_SQN34X0-GECKO_LR8.0.0.3-52148.tgz

  Containing the needed *Python* script

Unpack the packages as follows:

```
tar xzf GM02_BIN_SQN34X0-GECKO_LR8.0.0.3-52148.tgztar xzf RYZ024A_LR8.0.0.3-52148.tgz

mv RYZ024-SDK RYZ024-SDK-8.0.0.3-52148 // This is to avoid the next step undo the previous one.

tar xzf RYZ024A_LR8.0.0.3-52128.tgz

mv SEQUANS-SDK SEQUANS-SDK-8.0.0.3-52128 //As above, this is to avoid being overwritten by any other decompression
```

Then build the needed libraries:

```
cd RYZ024-SDK-8.0.0.3-52148/bin/

//build sqnbsdiff manuallymake -C
sqnbsdiff

//go back to RYZ024-SDK root pathcd ..
```

The following steps are optional; they are done to simplify the commands afterwards.

```
cp ../RYZ024-SDK-8.0.0.3-52128/platform/renesas/ryz024a/ue/SQN3430/ue.dup

./ue_52128.dup

cp ../RYZ024-SDK-8.0.0.3-52128/platform/renesas/ryz024a/updater/SQN3430/
updater.dup ./updater_52128.dup

cp ../RYZ024-SDK-8.0.0.3-52128/platform/renesas/ryz024a/filesystem/
GENERIC/filesystem.dup ./filesystem_52128.dup

cp ./platform/renesas/ryz024a/ue/SQN3430/ue.dup ./ue_52148.dup

cp ./platform/renesas/ryz024a/updater/SQN3430/updater.dup ./
updater_52148.dup

cp ./platform/renesas/ryz024a/filesystem/GENERIC/filesystem.dup ./
filesystem_52148.dup
```

Then the tool `upgrade-gen.py` generates differential images for each part of thefirmware and collects them.

`upgrade-gen.py -h` outputs the script's usage. For differential image generation, the mandatory options are:

`-t <type>`

Indicate which part of the firmware you want to generate:

`updater` – for the updater part

`fff` – for the firmware part

`fs` – for the file system part

`-c <bootrom_config>.py`

The bootrom configuration file. This piece comes from the platform package, it contains the definition of the flash partition

`-d <DIFF>`

The original image already flashed on the device

The supported formats are elf, dup, img.

`-f <FILE>`

The target file to be upgraded to. The supported formats are elf, dup, img.

`-o <DIFF-to-FILE>.dup`

The name of the output differential image in dup format.

(1) Differential Updater Generation

Run the following command to generate the differential updater part (in a dup format).

```
./bin/upgrade-gen.py -t updater -c ./platform/renesas/ryz024a/bootrom/
SQN3430/RYZ024A.py -d ./updater_52128.dup -f ./updater_52148.dup -o
updater_52128-to-52148.dup
```

(2) Differential UE Firmware Generation

Run the following command to generate the differential UE firmware part (in dup format).

```
./bin/upgrade-gen.py -t fff -c ./platform/renesas/ryz024a/bootrom/SQN3430/
RYZ024A.py -d ./ue_52128.dup -f ./ue_52148.dup -o ue_52128-to-52148.dup
```

(3) Differential Filesystem Generation

Run the following command to generate the differential filesystem part (in dup format).

Since there is no difference in the file systems of these two firmware versions, the size of the output file is 0.

```
//Add $PWD/bin/yaffs/utils in your PATH export PATH=$PATH:$PWD/bin/yaffs/utils/
```

```
./bin/upgrade-gen.py -t fs -c ./platform/renesas/ryz024a/bootrom/SQN3430/
RYZ024A.py -d ./filesystem_52128.dup -f ./filesystem_52148.dup -o
filesystem_52128-to-52148.dup
```

(4) Differential dup Image with Multi Sub dup Images Generation

You can then collect whatever DUPs parts you want into a full DUP image.

The example shows how to generate a differential DUP image including both the differential UE firmware and differential file system parts.

```
./bin/upgrade-gen.py pack -o diff-ue-updater_52128-to-52148.dup ue_52128- to-
52148.dup updater_52128-to-52148.dup
```

3.2.3 Device or Network Initiated FOTA

FOTA (Firmware Upgrade Over the Air) can be either device or network initiated using LwM2M. In both cases, the connection manager must ensure that the device's battery level is high enough before triggering or accepting a FOTA upgrade.

3.2.3.1 Device-Initiated Firmware Upgrade

The connection manager launches the FOTA using proprietary AT command `AT+SQNSUPGRADE`. Please refer to *Uses cases with AT commands* document for more details. The modem sends several URCs along the upgrade. The connection manager completely controls the upgrade process, modem reboot and connectivity.

The connection manager must not reset the modem during the upgrade.

During the asynchronous upgrade, the module first downloads the software image from the server and applies it at the next reset (booting is slightly longer). The reset can be triggered either by hardware, a software command or a software crash. The connection manager should therefore monitor both:

- The `+SHUTDOWN` URC sent after a software reset with AT^RESET
- The `^EXIT` message sent after a software crash

3.2.3.2 Network-Initiated Firmware Upgrade

The network relies on the LwM2M protocol to carry out a FOTA.

Both out-of-band (the LwM2M server instructs the LwM2M client to fetch a firmware image from a dedicated server) and in-band (the LwM2M server uploads the firmware image to the LwM2M client) FOTA are supported. In either case, the LwM2M client automatically performs the firmware upgrade as soon as it is notified by the LwM2M server.

Sequans LwM2M client supports two different bootstrap procedures:

- Factory Bootstrap
- Client Initiated Bootstrap

The Bootstrap Prioritisation Sequence works as follows: first, the LwM2M client registers to the Device Management server. If the server is unreachable, the client retries after a back-off period. The timing depends on the active operator mode:

- In Standard and Verizon operator modes, the LwM2M retries to connect 120, 360, 720 and 1200 s after the initial attempt
- In ATT operator mode: 720 and 1440 s

If the connection still fails, the LwM2M client launches a bootstrap procedure.
The modem informs the MCU on the upgrade’s progress using `+SQNSUPGRADE` URCs. These URCs are disabled by default and must be activated, when LwM2M is enabled, using `AT+SQNSUPGRADECFG`.

```
AT+SQNSUPGRADECFG=0,1,10
OK
+SQNSUPGRADE: "available"
+SQNSUPGRADE: "downloading",0
+SQNSUPGRADE: "downloading",100
+SQNSUPGRADE: "downloading",100
+SQNSUPGRADE: "rebooting"
+SYSSTART
```

The connection manager must not reset the modem during the upgrade.

4. Factory Reset

If the modem shows erratic behavior such as crash loops or repeated disconnections for no apparent reason, the MCU may have to perform a factory reset with the command `AT+SQNSFACTORYRESET.`

After a factory reset, the MCU must reconfigure the device. The LPM settings, the file system and the PSI (platform specific information, such as the UART configuration) need to be restored.

Factory resets can be triggered by the network using LwM2M. There is no URC sent to warn the MCU of an incoming factory reset. Therefore, the MCU must check the configuration of the device every time a reboot is detected (`+SYSSTART URC`). LwM2M support is mandatory and is automatically activated when the modem enters the following operator modes: Verizon, AT&T and Softbank (see section 2.2.1, Operator Modes).

LwM2M support is mandatory and automatically activated when the modem is in the following operator modes (`AT+SQNCTM`): Verizon, Verizon non-roaming and AT&T(see section 2.2.1, Operator Modes).

5. Abbreviation

DCE	Data Communications Equipment
DTE	Data Terminal Equipment
URC	Unsolicited Response Code
BIP	Bearer Independent Protocol
CTS	Clear Tp Send
RTS	Request To Send
eDRX	Extended Discontinuous Reception
PSM	Power Saving Mode
UE	User Equipment
MCU	Microcontroller Unit
UART	Universal Asynchronous Receiver Transmitter
PPP	Point to Point Protocol
SMS	Short Message Service
SMSC	SMS Center
GPIO	General Purpose Input Output
RRC	Radio Resource Control
PMU	Power Management Unit
LTE	Long Term Evolution
APN	Access Point Name
PDN	Packet Data Network
PLMN	Public Land Mobile Network
EARFCN	E-UTRA Absolute Radio Frequency Channel Number
IMEI	International Mobile Equipment Identity
IMSI	International mobile subscriber identity
HLR	Home Location Register
FOTA	Firmware Over The Air
TAU	Tracking Area Update
LwM2M	Lightweight Machine to Machine
PER	Packet Error Rate

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Sep.29.22	-	First release

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.

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

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/.