SARA-R42

Application development guide
Application note

Abstract

This document provides detailed technology architecture and examples of how to use AT commands with u-blox SARA-R422 / SARA-R422S / SARA-R422M8S modules.

Document information

Title	**SARA-R42**	
Subtitle	Application development guide	
Document type	Application note	
Document number	UBX-20050829	
Revision and date	R02	09-Jul-2021
Disclosure restriction	C1-Public	

This document applies to the following products:

Product name
SARA-R422
SARA-R422S
SARA-R422M8S

Contents

1 Introduction

This document provides a wide guidance for developing applications that interface with the u-blox SARA-R422 / SARA-R422S / SARA-R422M8S modules, including AT command sequences examples for specific use cases. Throughout the document, "SARA-R42" represents any of these modules.

This should be the first document to read when working on an application integrating a SARA-R42 module. Section 2 starts with a generic overview of the supported cellular technologies. Then, it describes the basic application design steps to follow when integrating the SARA-R42 module (section 3) and some details about the AT command parser (section 4), which is a very important component of the application. Next, it provides information on fundamental topics specifically related to SARA-R42, such as local connectivity (section 5), MNO profiles (section 6), network registration (section 7), power saving mode and eDRX (section 8). As another important functionality, an application should include is monitoring the module status and reacting to possible issues in the correct way: details about this can be found in section 9. Section 10 describes how to use the `+UTEST` AT command for OEM production testing and its possible configurations.

Other application notes are available to delve into specific topics, they are referenced in section 11.

Finally, a list of software changes with respect to SARA-R410M / SARA-R412M is provided in section 12 and can be useful when migrating an application from SARA-R410M / SARA-R412M to SARA-R42 modules.

Table 1 shows a summary of the documentation available for SARA-R42.

	Document name	Notes
Application integration	Application development guide app note	This document. **Start here!**
	FW update app note [4]	FW update procedures (uFOTA, FOAT, FOTA, +UFWINSTALL, EasyFlash).
	Internet applications development guide app note [5]	Any applications relying on the IP stack (sockets, MQTT, MQTT-SN, HTTP, FTP, CoAP, SSL/TLS).
	IoT Security-as-a-Service app note [6]	IoT-as-a-Service features (local encryption, E2E encryption, E2E symmetric KMS, Chip-to-Chip, Zero Touch Provisioning).
	GNSS implementation app note [7]	GNSS interface and aiding clients. Techniques for hybrid positioning and timing indication.
	LwM2M application note [9]	Details about the LwM2M options to achieve a few mandatory objects, extensible object and Firmware Over The Air update (uFOTA).
	AT command connect to AWS IoT core [10]	Examples of how to use AT commands in order to properly interact with the AWS IoT service.
	Mux implementation app note [8]	Usage of multiplexer with cellular modules.
	EVK-R4 user guide [11]	Starting guide for the SARA-R4 evaluation kit.
Reference documentation	Data sheet [1]	Use these documents as hardware integration and AT commands API reference.
	System integration manual [3]	
	AT commands manual [2]	
Product release documents	Sample Delivery Note / Information Note	Delivered with every FW release.

Table 1: SARA-R42 documentation overview

See SARA-R4 series AT commands manual [2] for detailed AT command descriptions.

The following symbols are used to highlight important information within this document:

☞ An index finger points out key information pertaining to module integration and performance.

⚠ A warning symbol indicates actions that could negatively impact or damage the module.

2   Cellular technology overview

SARA-R42 modules support LTE Cat M1 and NB-IoT as LPWAN technologies plus the 2G RAT as fallback, such as used in application areas:

- Automotive and transportation
- Smart metering
- Smart cities
- Smart buildings
- Connected health
- Agricultural and environmental

2.1   Radio Access Technologies (RATs)

2.1.1   LTE Cat M1

LTE Cat M1 is a low-power wide-area (LPWA) air interface that enables the connection to IoT and M2M devices with medium data rate requirements. It increases battery lifespans thanks to enhanced power saving mode and extended in-building range (up to 15 dBm more than LTE, thanks to the repetitions of transmissions provided in the Coverage Enhancement modes), as compared to standard cellular technologies such as 2G, 3G, or LTE Cat 1.

LTE Cat M1 is defined by the 3GPP Release 13 and is a LPWA technology operating in the licensed spectrum. Operating in half duplex mode with typical speeds of 375 kbit/s, which can reach 1 Mbit/s on some networks thanks to protocol stack enhancements, LTE Cat M1 specifically supports IoT applications with low to medium data rate needs. At these speeds, LTE Cat M1 can deliver remote firmware updates over-the-air (uFOTA, with access to MNOs and u-blox servers via the LwM2M protocol) within reasonable timeframes, making it well-suited for critical applications running on devices that may be deployed in the field for extended periods of time.

As M stands for mobility, the LTE Cat M1 standard specifies Connected Mode Mobility, which the module supports through inter-frequency and intra-frequency handover capability, resulting in higher reliability of transmissions, particularly important in non-static usage.

2.1.2   NB-IoT

Narrowband IoT (NB-IoT Internet of Things) is a Low Power Wide Area (LPWA) technology standardized by 3GPP release 13 as a specialization of the LTE standard, operating with 200 kHz bandwidth which allows it to work virtually anywhere. Since it operates in licensed spectrum, it is secure and reliable, providing guaranteed quality of service.

NB-IoT is optimized for applications that need to communicate small amounts of data over long periods of time. Similar to Cat M1, it offers very low power consumption and excellent extended coverage in buildings and underground. Battery life of up to 10 years on a single charge in some use cases also contributes to lower maintenance costs for deployed devices, even in locations where end devices may not be connected directly to the power grid.

SARA-R4 series modules support both CP (Control Plane) and UP (User Plane) Cellular IoT EPS optimizations, Cat-NB2 (3GPP Release 14 upgraded version of the NB-IoT standard, which increases the maximum bit rate from ca 30-60 kbit/s to up to 120-160 kbit/s), NAS and AS (Access Stratum) RAI (Release Assistance Indicator) for faster release of the RRC connection at the end of the data transactions.

2.1.3 GSM/EGPRS

To assure global coverage, the module supports also 2G legacy RAT, more precisely it supports EGPRS class 33 with a downlink maximum speed of ~ 290 kbit/s (the peak bit rate depends on the quality of the radio link). Being a data-only device, in 2G RAT, besides performing GPRS attach, the module also registers for CS (Circuit Switched) services in order to enable the GSM SMS service. This is a major difference with respect to NB-IoT RAT, where often the SMS service is granted even if the LTE attach is accepted for EPS services only, thanks to the "SMS only" option negotiated during the LTE attach. Another major difference is the fact that the host application needs to establish a PDP context activation in order to get an IP address and be able to use the module's IP based applications.

2.2 Low power profile features

When integrating SARA-R4 series modules in a low power consumption device, it is recommended to enable the power saving mode via +UPSV AT command. Depending on the configuration of the serial line used, different +UPSV modes can be selected (see the SARA-R4 series system integration manual [3] and the SARA-R4 series AT commands manual [2]).

To benefit from the enhancement of the LPWA standards, the power saving mode (PSM) can be enabled too. In normal service in LTE Cat M1 and NB-IoT, during inactive phases the PSM feature forces the module to enter a low power mode state, where the module is totally deactivated. The state is exited either if the host application needs to trigger data or AT commands, or when the device has to perform the periodic registration to the LTE network, which in PSM is done less frequently than in normal, non-PSM operational mode (for example, after a few hours). Overall, this behavior is more convenient with respect to usage of on-demand radio switch off/on via AT+CFUN=0/1 but has the disadvantage of long-lasting non-reachability periods while the device is deactivated. Similarly, host applications using mobile-terminated user data (for example, SMS) can rely on eDRX (extended DRX) to keep the power consumption at an optimal level while retaining reachability.

SARA-R4 series modules assure enhanced coverage thanks to the support of CE (Coverage Enhancement) modes A and B; this benefit is balanced by longer transmission duration due to the several repetitions, which the host application can mitigate by using a reduced transmission duty cycle for optimal tradeoff.

3   Application design and development

When designing a host application interfacing with a u-blox cellular module, consider the following points, as depicted in Figure 1:

- Choose the module's features that the application needs, and the ones that can be disabled.
- Split the application workflow into stages.
- Design the application to work in several modes, reflecting the lifecycle steps of the product.
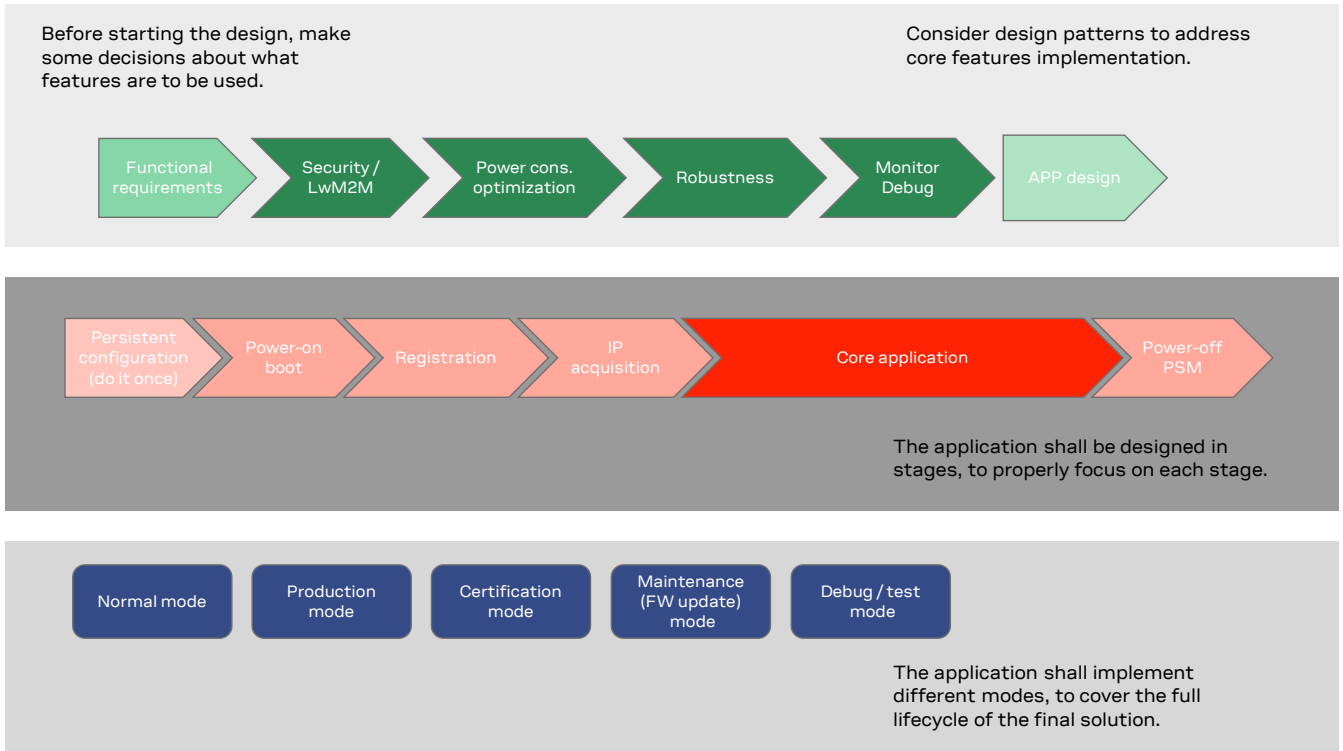
Figure 1: Application design

3.1   Initial design decisions

If some features will never be used during the application lifetime, they should be disabled or properly configured in order to minimize their impact on the overall performance. These decisions should be carefully taken at design stage, because later changes can cause much effort to adapt and validate the application.

These decisions concern:

- Usage of an LwM2M client
- Usage of security suite features
- Usage of power saving
- SIM card/MNO selection
- SW/HW monitor and debug solutions
- SW/HW recovery modes

An LwM2M client is necessary so that MNOs can contact the device and retrieve diagnostic information; it also enables automatic periodic checking of FOTA update availability, on both MNO and u-blox servers. Based on the target power consumption profile, the customer application can periodically enable the client to control features, such as the periodic LwM2M registrations with the server, or it can implement alternative or additional methods to implement FW updates when triggered by prolonged out of service conditions or by specific events.

Similar considerations hold for the security client.

Power saving features (+UPSV, PSM, eDRX) shall be configured based on the target power consumption profile, based on the suggestions in section 8.

The MNO profile (section 6) to be used depends on the type of application and SIM card (regional or global roaming). If the SIM card belongs to an MNO for which the module has gained the type approval, the MNO profile is available in the FW and shall be used. For more details about this, see the SARA-R4 series data sheet [1].

Debuggability can be provided via test endpoints, access to the USB interface, and in general a prolific application log containing all AT command strings exchanged with the module and diagnostic information sent by the module with timing information. Monitoring the module status is a requirement to implement recovery procedures via HW or SW, as described in section 9.

☞ To evaluate the disabling of the LwM2M client, especially in the scenarios in which the related features are not explicitly required by the MNO and not needed by the user.

3.2 Application stages

3.2.1 Persistent configurations

Some module settings are persistent, that is, they are stored in the module Non-Volatile Memory (NVM). Among these are the MNO profile (see section 6), APN for Internet connectivity, and active LTE bands.

The host application should implement a persistent configuration setting phase, performed once and then at an as-needed basis, where all AT commands related to the required settings are issued.

☞ See the SARA-R4 FW update application note [4] for persistence of settings after a FW update. If settings are not retained, they shall be reapplied as per section 3.2.2.

3.2.2 Power on/boot/PSM exit

In general at each boot, the application should read configurations and make sure they are correct. If not, persistent configurations can be reapplied.

Not all the module configurations are persistent. Therefore, the application, after each module boot, should again set these volatile configurations (for example, AT+CMEE=2, URC enabling).

It is very important that the application has a robust mechanism to detect when the module is ready to communicate via AT commands at the power-on: a solution is to enable the greeting message (+CSGT AT command); alternatively, the host application can wait for a response to "AT" command.

The application should configure module time. Automatic update of local time with the network time information is the factory setting (+CTZU: 1), so after LTE attach, the time of the module is generally updated.

☞ When using PSM, at exit from low power mode, the volatile settings as well as the current communication port mode (MUX, dialup) shall be restored too.

3.2.3 Network registration

For details about the network registration stage, see section 6.

3.2.4 IP acquisition

For some details and guidelines on this topic, see the Internet applications development guide application note [5].

3.2.5 Core application

For some details and guidelines on this topic, see the Internet applications development guide application note [5] and SARA-R4 series AT command manual [2]. The application shall handle AT commands, responses and unsolicited indications as suggested in section 4. For diagnostic purposes, the application should rely on status AT commands, see section 9.1. For robustness purposes, the application should implement embedded watchdog procedures, see section 9.2.

3.2.6 Power-off

The application might need to switch off the module; both normal and emergency shutdown are described in the SARA-R4 series system integration manual [3].

3.3 Application modes

An application is usually designed based on the main use cases in actual scenarios. This way of operation is what we call "normal mode". In addition, the designer should provide a way to configure the application for more specific contexts, which can have different requirements with respect to normal mode and can help to perform other important steps in the product lifecycle.

3.3.1 Debug / test mode

In general, an application should always output a significant log, including the AT commands it issues and their responses, and implement monitoring strategies as described in section 9.

If a problem occurs related to the cellular module and more information is needed, it may be necessary to configure different verbosity levels for the host application and modules log. This can be done with configuration files, that can be side-loaded to the file system. In extreme cases, it may be necessary to provide an AT interface passthrough to allow access to diagnostic AT commands.

If the cellular communication is tested against a network simulator, use a suitable test SIM card (usually provided by the network simulator manufacturer). If a test SIM card is not available, make sure to disable authentication and integrity checks on the tester side (by proper setting) and on the module (by using the AT+UDCONF=81,0 command, see SARA-R4 series AT commands manual [2]).

3.3.2 Production testing

This mode is to be used during the production tests of the end device. In this scenario the main application is usually inactive, and AT commands can be used to properly configure the module and use its end user testing features (see section 10).

3.3.3 Certification mode

Depending on the kind of certification, such as regulatory, conformance or for MNO type approval, the application might be disabled, and the module externally controlled (for example, for throughput testing). Specific MNO tests might require the application to be running in normal mode (for example, remote SIM provisioning, FOTA).

3.3.4 Firmware update mode

A module's firmware update should be implemented when necessary, either over the air or tethered. Each update strategy has its requirements and correct implementation, which should be followed to guarantee the success of the operation. See the SARA-R4 FW update application note [4] for more details.

4 AT commands response parser

It is important that the user implements a dedicated AT parser component in the host application.

Basic guidelines:

- When entering AT commands, spaces are ignored.
- The DTE shall handle the case of unexpected spaces or line endings, i.e. the <CR><LF> characters.
- As suggested in the SARA-R4 series AT commands manual [2], always wait for at least 20 ms following a final result code or a URC reception before issuing a new AT command.
- When the module has finished processing an AT command, it will output a final result code (either OK or ERROR) indicating that it is ready to accept a new AT command. The information text responses are issued before the final result code. Change +CMEE setting to numeric or verbose value (for example, AT+CMEE=1 or AT+CMEE=2).
- Asynchronous commands (for example, +UMQTTC) return an immediate final result code and final result via URC.
- Some AT commands return an intermediate result code (IRC) during command execution.

☞ Due to interface restrictions, when using multiple AT command interfaces, the parser should take into account that in SARA-R42 series it is not possible to have parallel activity on two or more AT terminals. Basically this behavior can be detected in the following configurations:

- o double UART availability, i.e. +USIO:1;
- o virtual channels set through multiplexer (MUX).

The only allowed parallel activity is present when it is defined a system architecture with a PPP dial-up on one port and AT commands on the other one.

4.1 Operational modes of the AT interface

When implementing the AT parser, it is important to consider that the communication port, whether the main UART or a MUX virtual port, enters different operational modes while processing AT commands.

In command mode, the module (called DCE – data communication equipment) can receive AT commands. Once an AT command is detected on the AT interface, the DCE processes it and may return to command mode by issuing a success or error response. Special AT commands lead the AT interface into intermediate states where, for example, an SMS payload is expected, or raw/binary data is exchanged (for example, during file transfer), or PPP packets are exchanged. In the latter case, the PPP data mode can be temporarily exited by a special +++ packet or DTR line ON-to-OFF transition and the online command mode (OLCM) state is entered: from this state, which is similar to the command mode, the DCE can be moved back to PPP data mode via ATO command or can disconnect PPP via ATH command (having previously applied AT+CVHU=0 as mandatory setting).

Figure 2 depicts the various modes in which the module can operate and shows the actions that cause transitions between the different modes. The transitions triggered by DTR line changes are configurable with the AT&D command, see SARA-R4 series AT commands manual [2].

For more details about the AT command interface settings, see the AT command settings section in the SARA-R4 series AT commands manual [2].
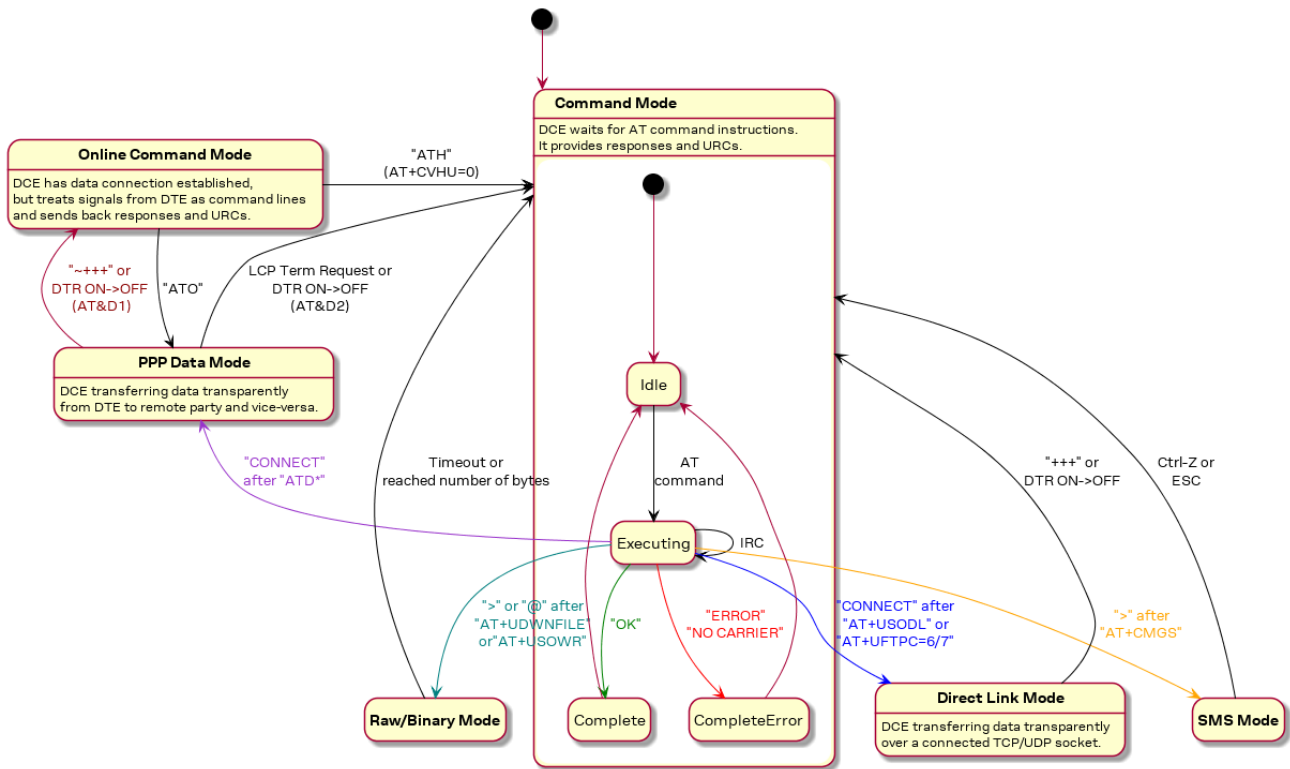
Figure 2: Module operating modes and actions causing mode transitions

4.2 Unsolicited result code

An unsolicited result code (URC) is a string message (provided by the DCE) that asynchronously indicates the occurrence of an event that might be related to a previous AT command or to the feature the user is currently using, or to the module's autonomous activity (for example, due to mobility).

When enabled on a given AT port, the URC can be output at any time to report a specific event or status change on the same AT port. If the AT port is busy, the application can decide to discard +CIND, +CGEV and SMS related URC by properly configuring the related AT commands; all other URCs will be deferred and printed when the AT port returns into command mode.

☞ Due to race conditions in mode transitions, URC can be received after an AT command has been transmitted by the host application.

Examples of some URCs are shown in Table 2.

URC	Description
+CEREG: <stat>[,<tac>,<ci>,<AcT>]	Network registration status or location has been updated
+CGEV: ME PDN ACT <cid>[,<reason>[,<cid_other>]]	The MT has activated a primary PDP context
+ULWM2MSTAT: <event>,<param1>[,<param2>]	LwM2M URCs generic syntax
+UUSOCL: <socket>	Socket has been closed

Table 2: URCs examples

5 Local connectivity

5.1 Serial interface configuration

It is possible to switch between 3 serial interface configuration variants, using the command `+USIO` AT command, as shown in Table 3.

Command	Response	Description
AT+USIO=0	OK	(Default configuration) AT on UART (9-wire: RXD, TXD, CTS, RTS, DTR, DSR, DCD, RI, GND), trace on USB.
AT+USIO=1	OK	AT on UART and AUX UART (5-wire: RX/TX, HW flow control, GND), trace on USB.
AT+USIO=4	OK	AT on UART (5-wire: RX/TX, HW flow control, GND), GNSS tunneling on AUX UART (5 wire: RX/TX, HW flow ctrl, GND), trace on USB.

Table 3: USIO variants description

☞ Reboot the module to apply the new USIO configuration. For more details on `+USIO` AT command, see the SARA-R4 series AT commands manual [2].

☞ `AT+USIO=4` option is not supported by SARA-R422 modules.

☞ URCs are sent to both UART and AUX UART interfaces when the `AT+USIO=1` option is set.

☞ It is not possible to have parallel activities on both AT terminals when the double UART configuration is selected, i.e. in `AT+USIO=1`. The only allowed parallel activity is present when it is defined a system architecture with a PPP dial-up on one port and AT commands on the other port.

☞ The `+URINGCFG` AT command is not applicable when the `AT+USIO=1` option is selected due to the fact that the RING line is not available at UART level in this configuration.

5.1.1 Auxiliary (AUX) serial interface configuration

If the AUX UART interface is enabled via the `+USIO` AT command as described above, then it may be necessary to properly configure this serial interface from the main UART interface, especially for the first use and in all cases when the factory-programmed configuration does not match the desired settings.

☞ Configuration changes are stored in the NVM and applied to the AUX UART interface at the next module boot.

The `+UUARTCONF` AT command applies the desired settings: some examples are reported in Table 4; for additional details, see the SARA-R4 series AT commands manual [2].

Command	Response	Description
AT+UUARTCONF=1,115200,3	OK	Set the desired baud rate and flow control mode for the auxiliary UART interface.
AT+UUARTCONF?	+UUARTCONF: 0,115200,3 +UUARTCONF: 1,115200,3 OK	Check the current settings for both the main UART and the auxiliary UART interfaces.
AT+UUARTCONF=?	+UUARTCONF: 1,(300,600,1200,2400,4800,9600,14400,19200,38400,57600,115200,230400,460800,921600,1000000,1200000,1500000,2000000,3000000),(0-3) OK	Visualize the possible settings to be applied in the auxiliary UART handling.

Table 4: +UUARTCONF variants description

☞ The "Set" command is available only for the auxiliary UART interface.

☞ The "Read" command is available for both the main UART and the auxiliary UART interfaces.

5.2 AT interface

AT commands can be issued to the module only via UART interface.

By default, the UART data rate is set to 115200 b/s, while "autobauding" is not supported by SARA-R4 series modules.

5.2.1 Set a fixed baud rate

Use the +IPR AT command to set a different baud rate for the main UART interface as shown in Table 5.

Command	Response	Description
AT+IPR=57600	OK	Set UART speed to fixed value 57600 bit/s. Cellular module response is sent at 115200 bit/s, i.e. at the original baud rate value.
After the "OK" final result code, wait for at least 200 ms before issuing a new AT command, to guarantee proper baud rate reconfiguration. Then send commands at the speed just set (57600 bit/s in the example).		
The new selected baud rate is immediately applied, a device reboot is not needed.		
AT+IPR?	+IPR:57600 OK	Check the current baud rate

Table 5: Setting a fixed baud rate example

☞ The UART speed takes around 200 ms to reconfigure itself after a baud rate change through the +IPR AT command.

☞ To show a greeting text at module boot (+CSGT AT command), set the desired fixed baud rate beforehand by using the +IPR AT command. If active, the greeting text is shown at boot once, on any AT interface, the first time the TE sets the DTR line to ON state.

☞ If using the Direct Link mode in downlink, it is advisable to apply 460800 b/s as fixed baud rate.

5.3 Multiplexer (MUX)

SARA-R4 series modules support the multiplexer functionality on the UART physical link as defined in the 3GPP TS 27.010 [13]. This makes it possible to have multiple simultaneous sessions (virtual channels) over the single UART interface.

The following virtual channels are defined:

• Channel 0: multiplexer control.
• Channels 1 to 2: AT commands / data connection.
• Channel 3: GNSS data tunneling (NMEA).[1]

For further details about the usage of multiplexer with SARA-R4 series modules, see the Mux implementation in cellular modules application note [8].

☞ The UART interface takes around 200 ms to reconfigure itself after the multiplexer configuration through the +CMUX AT command.

---

[1] Not supported by SARA-R422 modules

☞ It is not possible to have parallel activities on AT terminals when the multiplexer is activated through the `+CMUX` AT command. The only allowed parallel activity is present when it is defined a system architecture with a PPP dial-up on one port and AT commands on the other port.

☞ URCs are sent to all available AT interfaces when the multiplexer functionality is applied.

☞ The multiplexer protocol is not supported in the configurations having the AUX UART interface enabled (for example, `+USIO: 1, +USIO: 4`).

5.4 Point-to-point protocol (PPP)

Data (PSD) calls are possible over both primary UART and auxiliary UART interfaces.

☞ If the double UART configuration is used, the full V24 modem lines are not supported. In this configuration, entering in OLCM or disconnecting the PPP connection via DTR line de-assertion is not possible.

☞ Issue the AT+CVHU=0 command to make ATH over Online Command Mode (OLCM) work, according to 3GPP requirements. If the module has a DUN/PPP activated and is in OLCM, the command deactivates the PPP and the associated PDP context (if possible).

Further information about PPP dial-up establishment can be found in the Internet applications development guide application note [5] and in the EVK-R4 user guide [11].

5.5 Generic guidelines

To properly configure local connectivity, the following steps shall be considered:

1. Set the required connectivity variant at first usage, via the `+USIO` AT command.
2. Configure the GPIOs based on the set variant (especially in reference to the RI line), via the `+UGPIOC` AT command.
3. Configure the power saving control mode based on the set variant, via the `+UPSV` AT command.

6 MNO profiles

MNO profiles provide a powerful and flexible method to configure the SARA-R4 series module to seamlessly work with the SIM of the selected network operator.

Using the MNO profiles the module is dynamically configured to use the proper bands, RATs, and the operator-dependent protocol stack settings needed to operate on the home network in full compliance with the mobile operator requirements.

With the MNO profiles, a customer application is not required to configure the module using complex and/or network-dependent parameters, but benefits from a "out of the box" solution that provides seamless connectivity while abstracting the complexity of managing individual network configurations.

Use the `+UMNOPROF` AT command to select a profile for the network operator. For more details on the +UMNOPROF AT command and the MNO profile settings, see the SARA-R4 series AT commands manual [2].

6.1 Using MNO profiles

To configure the module to use an MNO profile, first make sure the module is de-registered from the network, then select the profile using the ID number and finally software-reset the module. When the module reboots, it will configure itself to use the parameters specified by the MNO.

☞ The host application should specify an MNO profile. The default and factory-programmed MNO profile is 90 (global profile).

☞ Reboot the module by means of `AT+CFUN=15` command (or the equivalent `AT+CFUN=16`) to make the MNO profile active.

6.2 Modifiable parameters

MNO profiles configure the module with a set of parameters. Some of these parameters can be overridden by using AT commands:

* `+UBANDMASK`   Band mask
* `+CGDCONT`   APN and PDP type

If the host changes any of these parameters, they will be retained after a module reset; if the MNO profile is re-applied, after reboot the MNO profile specific settings will be restored to the factory-programmed setting.

☞ Usually the APN will be accepted also when in roaming, but bands might need to be enabled to search for alternative PLMNs.

After setting the MNO profile the application may want to also modify the Radio Access Technology list and Band Mask.
Possible reason for setting +URAT may include:
* Radio Access Technology is not deployed by network carrier yet in the area device is intended to run on. Therefore only enabling the desired RAT will reduce scan time when device is searching for the network
Possible reason for setting +UBANDMASK may include:
* Band(s) is not deployed by carrier yet in the area device is intended to run.
* Device is an area where it is interested in running on specific bands only
* Reducing the number of bands will reduce scan time when the device is searching for the network in out-of-service or limited-service conditions.

6.3   MNO profile setting examples

Do not: set the MNO profile while the module is registered (Table 6)

Command	Response	Description
AT+CMEE=2	OK	Enable verbose error result code.
AT+COPS?	+COPS: 0,0,"00101",7 OK	Module is currently registered.
AT+UMNOPROF=100	OK	Do not set MNO profile while module is registered.

Table 6: Wrong way of setting the MNO profile

Do: de-register the module before setting MNO profile, then reboot it to apply the setting (Table 7)

Command	Response	Description
AT+CFUN=0	OK	Turn-off radio functionality, the module will de-register.
AT+UMNOPROF=100	OK	Set MNO profile for Standard Europe.
AT+CFUN=15	OK	Perform a module reset. After reboot, the MNO profile 100 settings are applied.

Table 7: Correct way of setting the MNO profile

6.4   Global profile (+UMNOPROF: 90)

This is the default profile for the SARA-R422 / SARA-R422S / SARA-R422M8S modules, with all supported bands set as enabled on all available RATs (LTE-M, NB-IoT, GSM).

6.5   Standard Europe (+UMNOPROF: 100)

The MNO profile 100 should be used as the basis for all other MNOs in Europe outside of ones explicitly referred in other profiles. However, there may be changes that need to be applied to the module for proper operation with any given MNO such as attach type, RAT preference, band selection, etc. Please consult with the preferred network provider.

If the device is attaching to a network operator (even outside of Europe) that is not listed in the MNO profile list, MNO profile 100 should be used as a generic and configurable profile.

Also, it is recommended to use this profile for mobile virtual network operator (MVNO) and/or roaming SIMs.

6.6   GCF-PTCRB (+UMNOPROF: 201)

This MNO profile can be used during production or lab tests. With this profile, LwM2M is disabled.

6.7   SIM ICCID select profile (+UMNOPROF: 1)

It can be used by host applications that will use different SIM cards. In this setting the Mobile Network Operator profile is selected according to the SIM Issuer Identifier Number (IIN), whose ranges are predefined for each MNO profile.

If the IIN selection algorithm cannot find a suitable MNO profile for the given SIM card, then the global profile (+UMNOPROF: 90) is the selected as fallback.

A first reboot, triggered by the application, is necessary to activate the IIN automatic selection. A second reboot, again triggered by the application, is required to have the detected MNO configuration applied. See the SARA-R4 series AT commands manual [2] for details on the AT command and URC syntax and reboot configurability.

Table 8 shows an example of automatic MNO profile detection setting usage.

Command	Response	Description
AT+UMNOPROF=1	OK	Set the automatic MNO profile detection, the automatic reset and enable the related URC.
AT+CFUN=15		DTE is required to perform first reboot
AT+UMNOPROF?	+UMNOPROF: 1,0 OK	UMNOPROF is ready to perform automatic selection, another reboot is required.
AT+CFUN=15		DTE performs the second reboot
AT+UMNOPROF?	+UMNOPROF: 1,2 OK	Read the detected profile

Table 8: Setting automatic MNO profile detection example

7 Network registration

At power-on the module reads the information in the currently selected MNO profile. It will use this information to configure which bands to scan, the radio access technology to use if more than one is supported, and other attach parameters like APN.

Once the module has found a suitable cell it can camp on, it will start the registration process. Depending on the current PLMN, during the registration the device can be provisioned with the APN or the APN must be provided by the host application as part of the persistent settings.

A new SIM can be activated after its first registration on a real network: its "profile" (i.e. contents of the SIM files) can be remotely provisioned over the air and a registration cycle is triggered at the end of the SIM OTA procedure.

☞ PIN lock shall be disabled if the device is expected to work with PSM enabled.

7.1 Band configuration

The module can scan over several bands to find a network to attach to. The host application can limit the scanning to specific bands to shorten the time to find a network.

Use the +UBANDMASK AT command to specify these bands as an 8-byte bitmask. In the bitmask, the bit at (band-1) position enables (if 1) or disables (if 0) the scan of the band. Some examples are depicted in Figure 3.

Bands	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	SUM	BITMASK
Base 2	2^{27}	2^{26}	2^{25}	2^{24}	2^{23}	2^{22}	2^{21}	2^{20}	2^{19}	2^{18}	2^{17}	2^{16}	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}	SUM	BITMASK
Enable B20 only	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2^{19}	524288
Enable B2,B4,B5,B12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	$2^{11}+2^{4}+2^{3}+2^{1}$	2074
Enable B4, B13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	$2^{12}+2^{3}$	4104

Use these values for AT+UBANDMASK

Figure 3: +UBANDMASK bitmask creation examples

☞ Each MNO profile will define a set of bands to scan on.

7.1.1 Scan time

SARA-R4 series modules will scan each band configured for each RAT selected. By reducing the number of bands and selecting only one RAT, the module may attach to a network more quickly than if all bands are configured.

Because NB-IoT allows for cells to be found with much higher dynamic range, the scan time in NB-IoT is much longer than LTE Cat M1. If the application has configured NB-IoT as well as LTE Cat M1, but there are no NB-IoT networks, the module may take a couple minutes per band to complete the NB-IoT scanning before re-trying the LTE Cat M1 RAT scan. If a global roaming profile is used, the application can rely on the automatic band scan and PLMN search done by the device at national border crossings. Alternatively, to optimize power consumption and reduce the impact of band scan and PLMN searches in out of coverage situations, the application shall reduce the supported bands based on regional information provided by the module via AT command interface, and change bands with some hysteresis.

Regarding the possibility to perform network scans when the module is in automatic selection, i.e. AT+COPS=0, the following points have to be taken into account:

- the radio access technologies are considered accordingly to the +URAT AT command settings about the preference order (<1stAcT>, <2ndAcT> and <3rdAcT>);
- the preference order of the radio access technologies could be overruled by the +CPOL preferred operator list and the related <AcT>.

The described behavior has to be considered especially in roaming conditions.

7.1.1.1 OOS scan timings

The scan algorithm is implemented when attempting to gain service at power-up and when the out-of-service (OOS) condition is detected. A full system scan is interspersed with sleep intervals to reduce power consumption. The algorithm starts with a sleep time of 30 s which is applied 10 times, then the sleep time is incremented to 45 s, which again is applied for other 10 times, finally the sleep time is set to 60 s.

Each full system scan starts with the search of recently used cells, if available, which are coming from an internal database updated every time the device can find full service on a cell. Then the full system scan continues triggering a band scan for all enabled bands. At each step, the full scan considers all the enabled RATs ordered according to the configured relative priority. RAT and band settings can be configured with the +URAT and +UBANDMASK AT commands if not locked.

This algorithm is maintained until a suitable cell providing full or limited service is found and the device can camp on it.

To keep power consumption even lower, the recommendation is to implement an algorithm on the application processor to switch the device off if not able to gain service for a long period of time and then switch it back on after a while to try to get full service again. The duty cycle can be selected by the host application based on the tradeoff between power consumption and maximum tolerable delay before regaining cellular coverage.

7.2 First time registration setup

It is important to set the operator profile first because this operation will configure the default RAT and band mask for that corresponding profile. If the +UMNOPROF set command is issued after the +URAT or +UBANDMASK AT commands, then it will override any past configuration the host application has made. The module is programmed with auto-cops, so no AT command is required to trigger the network registration.

☞ AT+CFUN=0/1 can be used to trigger a registration cycle with switch-off detach (which does not need the DETACH_ACCEPT message from the network). A detach of type normal can be obtained with the AT+CGATT=0 command.

☞ The AT+COPS=2/0 cycle shall be used when looking for a more suitable PLMN, as per SIM settings related to the preferred operator list available through the +CPOL AT command.

☞ The AT+COPS=2/0 cycle triggers a high priority PLMN scan, so this cycle shall be avoided in roaming conditions.

7.2.1 PAP/CHAP

If PAP or CHAP authentication is to be configured, the +UAUTHREQ AT command shall be entered.

If the authentication is required on the initial default bearer, the setting shall be entered in de-registered state.

7.2.2 Change of PDN settings (APN name and PDP type)

To change the PDN settings for the initial default EPS bearer established during LTE attach, edit the <cid>=1 PDN by means of the +CGDCONT AT command, as shown in Table 9.

Command	Response	Description
AT+CFUN=0	OK	Turn off the modem radio so to de-register the module.
AT+CEREG=2;+CGEREP=2,1	OK	Enable a set of registration URCs.

Command	Response	Description
AT+CGDCONT?	+CGDCONT: 1,"IPV4V6","","0.0.0.0 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,2,0,0,0,0,0,0 OK	Read IP type and APN for EPS attach bearer.
AT+CGDCONT=1,"IPV4V6","custom_APN"	OK	Set APN name ("custom_APN" for example) and the PDP type ("IPV4V6" for example) for EPS attach bearer.
AT+CFUN=1	OK +CEREG: 1,"0001","01a2d001",7 +CGEV: ME PDN ACT 1	Turn on the modem radio. URCs indicate the registration status change.

Table 9: Change of PDN settings example

7.2.3   Attach types

All profiles use Combined Attach (CS & PS); if successful, both data and SMS services are allowed. If LTE attach is successful for EPS only services, still SMS can be supported (the so called "SMS only" case). If LTE attach is not successful for SMS, the module can try registration on a different RAT (e.g. 2G RAT).

The +USVCDOMAIN AT command can be used to change how the module attaches to the network if the factory-programmed attach type is not accepted by the network.

7.2.3.1   NB-IoT networks: ePCO handling

On NB-IoT, where CP CIoT EPS optimizations are mandatorily active, the 3GPP standard prescribes that the extended Protocol Configuration Options (ePCO) container is used in Network Access Stratum (NAS) messaging when attaching to an LTE network. Some NB-IoT mobile operators do not support ePCO container; therefore, if ePCO is used in the attach for such a network, this will result in lack of DNS capabilities, e.g. for NB-IoT networks that are known to not support ePCO or when +CGCONTRDP AT command does not return any DNS in NBIoT, it is recommended to use +UCFGCIOT AT command to disable the ePCO feature and fallback to PCO negotiation, as shown in Table 10.

Command	Response	Description
AT+COPS?	+COPS: 0,0,"NB-IoT Network",8 OK	Module registered on NB-IoT network.
AT+CGDCONT?	+CGDCONT: 1,"IP","default","192.168.20.2",0,0,0 OK	The module activated the EPS bearer with a valid IP address.
AT+CGCONTRDP	+CGCONTRDP: 1,5,"default","192.168.20.2","192.168.20.1","" OK	DNS references not available in the +CGCONTRDP AT command.
AT+UCFGCIOT=3,0	OK	Disable the ePCO feature through the +UCFGCIOT AT command.
AT+CFUN=15	OK	Reboot the module to apply the configuration.
AT+COPS?	+COPS: 0,0,"NB-IoT Network",8 OK	Module registered on NB-IoT network.
AT+CGDCONT?	+CGDCONT: 1,"IP","default","192.168.20.2",0,0,0 OK	The module activated the EPS bearer with a valid IP address.
AT+CGCONTRDP	+CGCONTRDP: 1,5,"default","192.168.20.2","192.168.20.1","185.215.195.114" OK	DNS references now available in the +CGCONTRDP AT command.

Table 10: ePCO feature disabling

7.2.4 Radio Policy Manager

SARA-R4 series modules implement the Radio Policy Manager (RPM) feature according to GSMA connection efficiency TS 34 [14]. RPM aims to prevent cellular devices to aggressively try registration or PDP context activation procedures in case of permanent failures (e.g. "invalid UE" or "EPS services not allowed"), which are usually due to subscription restrictions, in addition to standard 3GPP retry algorithms. Since these aggressive behaviors can cause network overload and service outage, some MNOs require to have RPM active by default: the RPM feature is enabled only on specific MNO profiles (for more details, see appendix C of SARA-R4 series AT commands manual [2]), but they can be enabled via AT commands on other MNOs requiring it.

7.2.4.1 Management of SW resets

In particular, RPM limits the number of user-initiated module resets per hour following a permanent attach reject cause; the AT commands which are controlled and can provide an error result code are the following: `AT+CFUN=15`, `AT+CFUN=16`, `AT+CFUN=19`, `AT+CFUN=1,1` and `AT+CFUN=4,1`, and `AT+CPWROFF`.

Eventually, RPM will again allow these commands and can even autonomously trigger a SW reset: timers and maximum counters can be derived from the MNO SIM card (so they can be even OTA updated) or are retrieved from the NVM (at most 1 module reset per hour is usually allowed per GSMA). RPM counters are cleared after a successful registration.

7.2.4.2 Management of PDP context activations

RPM also limits the maximum number of successful PDP context activations on the same APN (e.g. for Deutsche Telekom (DT) MNO the limit is 30), the maximum number of PDP context activations requests per hour following a PDP context activation request ignored by the network (e.g. for DT it is 60), rejected with a "permanent" or a "temporary" reject cause (e.g. for Deutsche Telekom they are 30 and 60 respectively).

If PDP context activation is blocked by RPM, the `AT+CGACT=1,<cid>` command will fail with an error result code and the dial-up on a non-active <cid> will not be established.

Since the LTE attach usually implies a PDN connectivity activation, also LTE registration cycles triggered, for example by `AT+CFUN=0/1`, are subjected to the same limitations (e.g. for Deutsche Telekom maximum 30 attach/detach cycle per hours are allowed), however once the limit is exceeded the module will not register to the network for the following hour and no specific error will appear.

7.3 +UMACQOSTMR timer configuration

The `+UMACQOSTMR` AT command allows configuration of a proprietary MAC layer timer that acts as an additional mechanism that can be enabled to ensure LTE network local RRC release and return to idle after prolonged RX and TX inactivity of the radio channel. It is referred to being an "additional back-up mechanism", since the RRC procedure would normally handle the local RRC release. However, if there is a rare instance that it does not release timely with a network, this mechanism provides added reliability. An optimal and timely local RRC release is important to ensure the proper handling of any potential inbound network pages.

For details on the default +UMACQOSTMR settings, see the MNO profiles section in the appendix of the SARA-R4 series AT commands manual [2].

When using network simulators, to perform certain types of measurements there may be a need to stay in local RRC connected state. See section 10.2 for details for guidance to disable the timer in such situations.

7.4 Registration monitoring

Use the `+CEREG` AT command to confirm the module is registered on the LTE network for LTE Cat M1 or NB1. Use `+CREG` and `+CGREG` AT commands for CS and GPRS network registration status.

When registering on an LTE Cat M1 or NB1 network the PDN context will be automatically created and activated; for 2G networks the host needs to manually activate the PDN context using the `+CGACT` AT command.

☞ Independently of the selected RAT, always issue the `AT+CGACT=1,<cid>` command on used context <cid> even if the `+CGDCONT` AT command returns that the context is still active with a valid IP address. This is highly recommended to activate the PS data connection avoiding possible conflicts between applications.

☞ If the uFOTA is enabled and needs to contact the uFOTA server when running on 2G RAT, the LwM2M will automatically activate the default context.

7.4.1 Detecting the access technology

SARA-R4 series modules can connect to different types of access technologies, i.e. LTE Cat M1, NB-IoT and GPRS. Because the modules can be configured to automatically connect to any of these access technologies, there are AT commands the host application can use to detect what technology is being used.

The best AT command to use is the `+COPS` AT command. The `+COPS` AT command has a `<AcT>` parameter which describes the access technology the module is registered to. However, this command does not provide a URC when the module is registered.

There are other AT commands that do have a URC when the registration is made. These also describe the access technology, i.e. `+CEREG` for LTE (Cat M1 or NB-IoT) and `+CGREG` (GPRS).

Host applications should always enable the URC for `+CEREG` and `+CGREG`. When the module registers on the network the application can read the access technology type from these URCs.

Basic operation would be:

Command	Response	Description
`AT+CEREG=1`	`OK`	Set URC for LTE
`AT+CGREG=1`	`OK`	Set URC for GPRS
<Wait for URC>		
`AT+COPS?`	`+COPS: 0,0,"Cat-M1 Network",7` `OK`	Read +COPS and check <AcT> parameter for RAT

☞ `+CREG` is used to describe if the module has been registered in the Circuit Switched Domain too for Combined Attach modes, accordingly it is advisable to enable the `AT+CREG=1` URC too.

7.4.2 PS connections at RAT change

When the module changes the RAT any PDP contexts and socket connections will be deactivated and disconnected. The host will need to re-create and re-activate socket connections. If the module had open sockets, the `+UUSOCL` URC will be issued when they are closed at RAT change.

LTE Cat M1 and NB1 networks, implementing the LTE standard, will automatically activate the default bearer PDP context, <cid>=1. Any other PDP context the host has configured and manually activated will have to be re-created and re-activated.

The 2G network may require the host to manual activate a PDP context as this is generally a manual procedure.

7.5   Mobility scenarios

Devices used in non-static installations can move out of range of the currently serving cell. This means entering another cell of the RPLMN (registered PLMN) or of a different PLMN or moving into an area where there is no cellular coverage or no roaming agreement for the device.

If the module loses the synchronization with the serving cell but finds another cell to camp on, any PDP context and open sockets will be kept. This holds in particular for seamless change of serving cell with cell reselection or handover procedures.

If mobility implies crossing national borders or simply changing the PLMN, it is likely that the new PLMN will force the module to reattach. This can also occur on the RPLMN, for example when the network needs to refresh IP addresses. If the module reselects a 2G cell and registers on a 2G PLMN, it is necessary to re-establish the PDP context in order to restore the services requiring cellular connectivity.

If mobility implies performing data traffic in roaming conditions, some aspects, such as the ones listed below, need to be taken into account in order to prevent possible undesired behaviors.

- Data sessions longer than 2 minutes
- Availability of an Operator PLMN (OPLMN) list with an entry of the same MCC as the current Registered PLMN

In this scenario, the module will carry out a high priority scan after 2 minutes, thus causing the abort of the RRC connection and the interruption of the data traffic.

A possible solution to this situation is to apply a manual PLMN selection as a workaround for this specific SIM setting.

Finally, if it is needed to limit data traffic when working in roaming conditions, the `AT+UDCONF=76` command could be referred applying the proper syntax. In this way the selected PDP context is not able to send data when roaming on a network.

7.5.1   Mobility Management procedures

Mobility management procedures are different depending on the state of the radio connection:

- Connected Mode Mobility (CMM) is handled by the eNodeB in LTE Cat M1. The UE is instructed by the eNodeB to provide measurement reports on neighbor cells so that the network can decide if and when the radio resource control (RRC) connection has to be handed over to another cell.
  - o The network itself will allocate gaps in the downlink transmission to allow the device to perform the intra-band or inter-band measurements: this will impact the downlink throughput.
  - o In case the eNodeB does not support CMM, or current RAT is NB-IoT or 2G, the RRC connection will be released at cell change due to radio link failure and it will be re-established by the device on the new selected cell. Radio link failures usually implies loss of uplink or downlink packets.
- Idle Mode Mobility is handled by the UE using information transmitted in the System Information Blocks (SIB) broadcast by the cellular network within the cell. While in idle mode the UE will make measurements of neighboring cells and based on the cell reselection criteria read in the SIBs it may choose another serving cell to synchronize with.

8 PSM, eDRX and deep-sleep mode

8.1 Power saving mode (PSM)

3GPP has a standardized PSM to minimize power consumptions for devices that require sporadic access to the cellular network. Instead of switching off the module at the end of the data transfer, if PSM is enabled with the +CPSMS AT command, then a device can negotiate long lasting time periods (up to 413 days) during which keepalive notifications can be postponed and the module can stay registered to the network.

Meanwhile, pending mobile terminated traffic indications, such as SMS or small data packets, are likely to be stored at the network side. This allows devices to skip paging reception and enter the minimum functionality PSM deep-sleep mode. To retrieve the pending mobile terminated (MT) traffic from the application server (AS), applications are suggested to implement a pull mechanism: the application client sends a mobile originated (MO) pull message to the server after the NW-buffered MT small trigger reception, the application server completes the MT data delivery upon the MO pull message reception.

The host application can preconfigure PSM on the module before registration or activate it at runtime (see the +CPSMS AT command description in the SARA-R4 series AT command manual [2]). The former solution is preferred because the second one triggers an extra PSM negotiation with the cellular network. The application-configured PSM settings are NVM persistent and used at any registration procedure, periodic or due to mobility in other areas, which is seen as a new negotiation opportunity. The requested PSM settings can be configured via the +CPSMS AT command, whereas the PSM settings assigned by the network, which are the used one, can be discovered via the +CEREG URC and the +UCPSMS AT command. If PSM is not granted by the network, then the module can not use PSM. In this case, for example, the host application could power on and off the module with the desired periodicity in order to save power.

Two timers determine the entrance into PSM deep-sleep mode, namely:

- T3324, the active timer, which starts when the network releases an existing RRC connection and is reset if a new RRC connection is established before the timer has expired. At T3324 expiry, the module can enter the PSM deep-sleep mode and it enters PSM deep-sleep as soon as the module completes any pending activity. If the eNB needs to send any MT data, then it always pages it before the active timer expiry. In case the eNB does not allow the UE to use PSM feature it does not grant it not assigning the active timer.
- T3412, the periodic TAU (Tracking Area Update) timer, which starts when the network releases an existing RRC connection and is reset if a new RRC connection is established before the timer has expired. It comes with two timer values: the legacy one and, in case of PSM, the optional extended timer value, used whenever present. By default, the cellular network sets the T3412 duration to almost 1 hour, but if PSM is supported, its duration can be extended to up to 413 days.

When PSM is granted by the network context retention is possible. At PSM deep-sleep exit no LTE attach is needed, previously activated EPS bearers and IP addresses are locally restored. The module can directly start a MO data or signaling transmission, e.g. a TAU procedure, when it exits PSM deep-sleep due to an early wake-up trigger or autonomously at periodic T3412 timer expiry.

8.1.1 GSMA recommendations

The selection of the requested T3412 timer value is a trade-off between power consumptions, which can be minimized setting long timer values, and the tolerated MT data delay, which is the limit factor for the T3412 timer duration. When using PSM it is recommended to request a T3412 timer extended value of at least 4 hours. In case no MT data is considered in the application design power can be minimized requesting the longest possible 413 days timer duration.

The selection of the requested T3324 timer value is a trade-off between power consumption and responsiveness. Low values save more battery life making it possible for the UE to enter PSM deep-sleep mode more quickly. High values of T3324 give some margin to the application server (AS) to respond to MO data sent by the UE before it enters PSM. AS responses to MO data can be both MO data acknowledgements as well as MT data delivery as a response to MO pull messages.

As a rule of thumb, the maximum suggested T3324 is 10 times shorter than T3412 and the minimum suggested T3324 should allow reliable paging if MT data or acknowledgements delivery is considered in the application design. The time needed to reliably deliver paging to the UE depends on whether the network uses discontinuous reception (DRX) and can be determined as 2*DRX cycle + 10 s (buffer time at network side), which amounts to 16 s in case of 2.36 s long DRX cycles. In case MT data or acknowledgements are not considered in the application design or in case the RRC inactivity timer adopted by the network matches the paging delivery reliability application needs a 0 s T3324 timer duration is also allowed.

Customers are advised to test out both parameters to come to a value that best fits their use case and requirements in terms of power consumptions, MT data delay, and reliability.

8.1.2 Timer values

8.1.2.1 Encoding of timer T3412

The extended TAU timer is encoded as GPRS timer 3 IE (see TS 3GPP TS 24.008 [12]).

Bits 5 to 1 represent the binary coded timer value. Bits 6 to 8 define the timer value unit for the GPRS timer and are encoded as follows.

```
BIT 8 7 6
    0 0 0 value is incremented in multiples of 10 minutes
    0 0 1 value is incremented in multiples of 1 hour
    0 1 0 value is incremented in multiples of 10 hours
    0 1 1 value is incremented in multiples of 2 seconds
    1 0 0 value is incremented in multiples of 30 seconds
    1 0 1 value is incremented in multiples of 1 minute
    1 1 0 value is incremented in multiples of 320 hours
    1 1 1 value indicates that the timer is deactivated
```

Example: "**010**00111" = 7 **x 10 hours** = 70 hours

☞ If the timer is not received in an integrity protected message (this can happen for example on lab setup on network simulators), the 110 unit shall be interpreted as 1 hour.

☞ If the 111 unit is used, the T3412 extended value is considered as not included in the message.

In case the network does not grant an extended periodic TAU timer value the standard periodic TAU timer value can be decoded using the T3324 timer table, since they share the same encoding. The standard or extended value encoding of the periodic TAU timer is indicated by the <Assigned_Periodic_TAU_Format_Type> parameter of the +UCPSMS AT command response.

8.1.2.2 Encoding of timer T3324

The Active Time T3324 is encoded as GPRS timer IE (see TS 3GPP TS 24.008 [12]).

Bits 5 to 1 represent the binary coded timer value. Bits 6 to 8 define the timer value unit for the GPRS timer as follows:

```
BIT 8 7 6
    0 0 0 value is incremented in multiples of 2 seconds
    0 0 1 value is incremented in multiples of 1 minute
    0 1 0 value is incremented in multiples of decihours (6 minutes)
    1 1 1 value indicates that the timer is deactivated
```

☞ All other values are to be interpreted as multiples of 1 minute.

Example: "**000**00100" = 4 **x 2 s** = 8 s

8.1.3   PSM and roaming

When the module is registered on a roaming network (not a home network), and the default "Automatic network selection" mode is enabled by the +COPS AT command, then the module will periodically search for a HPMLN (Home Public Land Mobile Network). HPLMN searches cause the module to exit PSM and delay PSM entry until the search is completed. If the device is roaming in "Manual network selection" mode, there are no HPLMN searches to impact the PSM feature.

8.1.4   Example of usage of PSM

Persistent settings

Command	Response	Description
AT+CFUN=0	OK	De-register the module.
AT+CEDRXS=0,4	OK	Disable eDRX in E-UTRAN (WB-S1 mode).
AT+UPSMR=1	OK	Enable the +UUPSMR diagnostic URC.
AT+CSCON=1	OK	Enable +CSCON diagnostic URC.
AT+CPSMS=1,,,"00111000" ,"00001010"	OK	Enable PSM deep-sleep mode and set the desired timer values (T3412(ext)=24 hours and T3324=20 s in the example).
AT+CFUN=15	OK	Reboot the module to apply the configuration.
AT+UPSMVER?	+UPSMVER:4,3,3,4,0 OK	Make sure the +UPSMVER AT command is set to its default value where PSM with context retention feature is enabled, otherwise enable it and start from the beginning.
AT+CPSMS?	+CPSMS:1,,,"00111000"," 00001010" OK	Check the +CPSMS AT command settings.
AT+CLCK="SC",2	+CLCK: 0 OK	Make sure SIM PIN check is disabled, otherwise disable it and start from the beginning.

Volatile settings

Command	Response	Description
AT+CEREG=4	OK	Enable the +CEREG URC with extended syntax to report negotiated PSM timer values. If issued in full functionality, the current status shall be queried via the +CEREG read command.

PSM in normal mode

Command	Response	Description
	+CSCON: 1	During LTE attach, the module is in RRC connected state.
	+CEREG: 1,"1","0","1",7, ,,"00001010","00111001"	During successful LTE attach PSM negotiation is performed. The +CEREG URC reports the PSM timer values assigned by the network, if any (T3324=20 s and T3412(ext)=25 hours in this case).
AT+CEREG?	+CEREG: 4,1,"1","0","1", 7,,,"00001010","00111001 " OK	Same information will be returned by querying the +CEREG AT command.
AT+UCPSMS?	+UCPSMS: 1,,,"00111001" ,"00001010",1 OK	The network assigned PSM settings are returned also by the proprietary +UCPSMS AT command, which provides the information whether PSM has been granted or not (+UCPSMS:0) and the granted PSM timer values in case it has been granted.

Command	Response	Description
	`+CSCON: 0`	At expiry of inactivity time on the network side, the RRC connection is released by the eNodeB. Both T3324 and T3412 timers are started with the assigned values.

	`+UUPSMR: 1,1`
	or
	`+UUPSMR: 2,3`
	`+UUPSMR: 1,1`
		At T3324 expiry the module can enter the PSM deep-sleep mode directly or with a delay as soon as it has completed any pending activity. The +UUPSMR URC allows to monitor the PSM deep-sleep mode entry.

	`+UUPSMR: 0`	At T3412 expiry the module exits the PSM deep-sleep mode to perform a TAU. The PSM deep-sleep mode exit can be also anticipated by the host application through an early wake-up via the PWR_ON pin. In both cases the PSM deep-sleep mode exit can be monitored via the +UUPSMR URC.
`ATD*99***1#`	`CONNECT`	At exit from PSM, PPP mode shall be locally restored. IP address will be the same assigned during attach, and uplink data can be sent to the network without the need to re-register.

8.2 Deep-sleep mode

In deep-sleep mode, enabled via `AT+CPSMS=1` command, the module keeps running at negligible current (for definitions and power consumption characterization, see the SARA-R4 series system integration manual [3]). The module is in minimum functionality, not responsive to AT commands. When the host application needs to interact with the module in deep-sleep state, e.g. to use the GNSS receiver, issue AT commands or to send MO data, it can either wait the module to exit deep-sleep state autonomously, e.g. at periodic T3412 timer expiry in case of PSM deep-sleep, or trigger an early wake-up via the PWR_ON pin. From a power consumption point of view the first solution needs to be preferred, if possible, for GNSS receiver usage and AT commands issuing, whereas the second one should be used for MO data, waking-up the module just before it exits PSM deep-sleep by itself when possible.

To keep power consumptions in deep-sleep extremely low the only running module component in this state is a low power low accuracy clock. Being this clock inaccurate, it can be affected by an always negative drift, causing the time in deep-sleep to be shortened by no more than 1% of the expected deep-sleep duration. When exiting deep-sleep the module checks the network time and, eventually, can immediately re-enter in deep-sleep if convenient from power consumption point-of-view.

When the module enters deep-sleep mode, it locally deactivates MUX and PPP and is not responsive to AT commands. Any non NVM saved settings are lost. Timers including application timers are reset except for T3412 and throttling timers: T3402, sever network failure (SNF, Verizon specific), T3346, T3396, and T3245 (if it is configured in USIM), which are saved and restored at deep-sleep exit. PIN check should not be used along with deep-sleep since it would prevent cellular connectivity restore at deep-sleep exit until PIN re-insertion. In case the autonomous wake-up would be scheduled in less than 1 minute the UE does not enter deep-sleep to compensate for boot penalty.

8.2.1 Deep-sleep aware applications and deep-sleep postponing

Some embedded applications and features can temporarily postpone entrance into deep-sleep mode until they have completed any pending activity. Activities that can delay deep-sleep mode entry are LwM2M, GNSS receiver usage and security, which might be waiting for a response from the server, as well as the AT interface, which restarts a 6 s guard timer any time a character is received over the UART interface. Deep-sleep aware applications preventing deep-sleep entry can be monitored via the `+UUPSMR:2,<client_id>` URC.

Coverage Extension (CE) modes can be another cause for entering deep-sleep with delay. In extended coverage the network may release the RRC connection later than in normal coverage to accommodate

the many retransmissions related to the Coverage Extension (CE) mode currently assigned to the UE. This can be checked via the +CEINFO AT command and the +CSCON URC.

IP based applications (e.g., MQTT, USOCK, UDNS, UFTP, HTTP) instead have no control on deep-sleep. They might be negatively impacted by the UE entering in deep-sleep state during the data sessions (such as UDP, TCP or secure sockets). This may happen in case the RRC connection is released and, in case of PSM deep-sleep, the T3324 expires while the UE is waiting for a network response. The network response delay can be a consequence of a temporarily server outage or packet loss in low coverage or mobility. This can be mitigated by the usage of UDP sockets instead of TCP ones, which also consumes less power. Like IP based applications, asynchronous AT commands, like +UMQTTC, have no control on deep-sleep which could be entered before the final result of the requested operation is received via URC.

In above cases the host application can temporarily postpone deep-sleep entry via the AT+UPSMVER=,,,,1 command (preferred solution) or keep issuing an AT command each time the AT interface guard timer is going to expire. To postpone deep-sleep entry during a blocking AT command execution, AT commands can be issued on another virtual AT port. When possible, deep-sleep temporary postponing is preferred to the disabling and re-enabling of deep-sleep via the +CPSMS AT command, which would waste power in two extra deregistration-registration cycles.

8.2.2   Deep-sleep indications

The host application can monitor the entrance and exit from deep-sleep state in several ways:

- GPIO "module status indication" (see the +UGPIOC AT command description in the SARA-R4 series AT command manual [2])
- V_INT monitoring
- RXD monitoring (if RXD is low for more than 1 character)
- +UUPSMR URC (printed on the AT interface when entering and exiting deep-sleep mode).

8.2.3   Deep-sleep state in out of service

The power efficient deep-sleep mode can be also entered in prolonged out-of-service conditions if the host application has enabled the minimum functionality PSM deep-sleep mode via the +CPSMS AT command. After a configurable number of unsuccessful full PLMN scans the module periodically enters the deep-sleep mode for 4 minutes before starting new network scans. Deep-sleep state in out of service can be tuned via the +UPSMVER AT command.

8.3   eDRX

SARA-R4 series modules support the 3GPP Release 13 feature Extended Discontinuous Reception (eDRX). This feature allows power consumption reduction, cyclically listening to paging without losing any paging indications. Paging is listened to only during short time periods (called PTW – Paging Time Windows) and ignored the rest of time. There is one PTW per the eDRX cycle. The application can enable eDRX feature negotiation via the +CEDRXS AT command. The command also allows configuration of the desired eDRX parameters: the requested eDRX cycle duration, also referred as TeDRX, and the PTW duration. If the network grants eDRX usage the assigned and finally used eDRX values can be read via the +CEDRXP URC and +CEDRXRDP AT command. It is suggested to deliver MT data with a pull mechanism already described for PSM. eDRX is commonly used on its own instead of PSM in applications where MT traffic is considered in the application design, a MT data delivery delay is affordable, but the tolerable delay is shorter than in PSM use cases. As a rule of thumb, eDRX is preferred to PSM when the maximum admissible MT data delay is shorter than the network T3412 duration, which has a default value of almost 1 hour. In this case, to minimize power consumption, it is suggested to set the requested TeDRX cycle duration as equal to the maximum affordable MT data delivery delay, and to set the requested PTW to the minimum duration, which makes paging reception

reliable. Customers are advised to test out both parameters to come to a value that best fits their use case and requirements in terms of power consumptions, MT data delay and reliability.

eDRX can be also used along with the PSM feature. In this case eDRX is used while the T3324 timer is running. When the UE tries to negotiate both PSM and eDRX features, the network interprets the request in the following way: if the requested TeDRX and T3412 extended values have similar durations then the network interprets that the UE would like to use eDRX or PSM, if the requested TeDRX cycle is at least one order of magnitude smaller than the requested T3412 extended value then the network interprets that the UE would like to use eDRX during the T3324 active time. In the latest case, for paging reliability, it is also advisable to request at least two TeDRX cycles during the T3324 active time (see Figure 4).
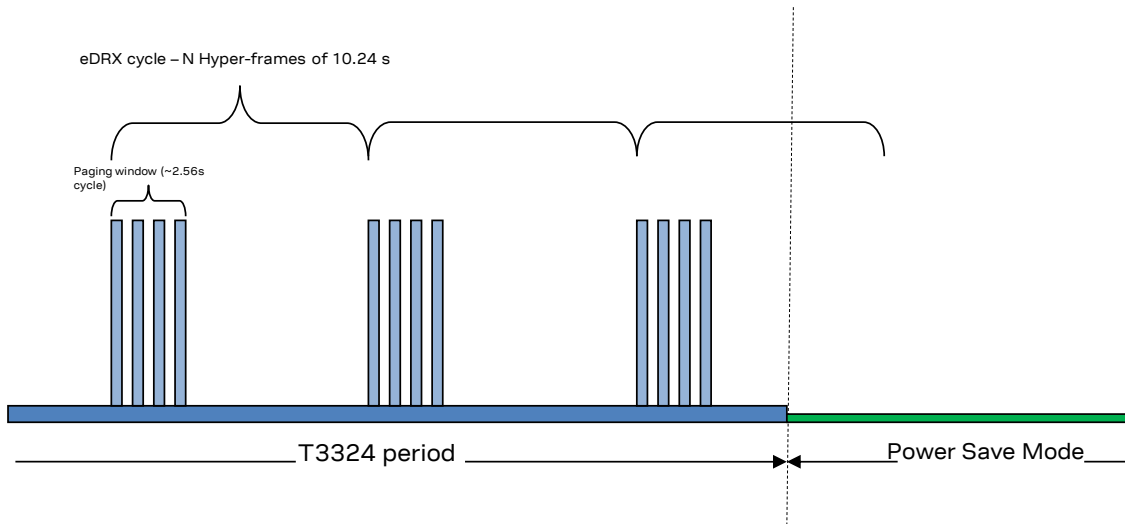
Figure 4: Paging listening when DRX, eDRX and PSM are enabled. In detail paging occasions are listened to during the eDRX PTW according to the network configured DRX cycle. eDRX is used during the PSM T3324 Active Time period.

8.3.1.1 Encoding of timer TeDRX

The TeDRX length, i.e. the requested eDRX cycle duration, is encoded as per Table 10.5.5.32/3GPP TS 24.008 [12]:

```
0 0 0 0        5.12 seconds
0 0 0 1       10.24 seconds
0 0 1 0       20.48 seconds
0 0 1 1       40.96 seconds
0 1 0 0       61.44 seconds
0 1 0 1       81.92 seconds
0 1 1 0       102.4 seconds
0 1 1 1      122.88 seconds
1 0 0 0      143.36 seconds
1 0 0 1      163.84 seconds
1 0 1 0      327.68 seconds
1 0 1 1      655.36 seconds
1 1 0 0     1310.72 seconds
1 1 0 1     2621.44 seconds
1 1 1 0     5242.88 seconds
1 1 1 1    10485.76 seconds
```

☞ All other values shall be interpreted as 0000.

☞ In LTE Cat M1 for the eDRX cycle length duration of 5.12 s the eDRX cycle parameter 'TeDRX' is not used.

☞ The 0000 and 0001 are only applicable in LTE Cat M1. If received in NB-IoT they need to be interpreted as if eDRX has not been granted by the network.

☞ The 0100, 0110, 0111 and 1000 values are only applicable in LTE Cat M1. If received in NB-IoT they need to be interpreted as the 0010 value.

☞ The 1110 and 1111 values are only applicable in NB-IoT. If received in LTE Cat M1 they need to be interpreted as the 1101 value.

8.3.1.2 Encoding of timer PTW

The PTW length is encoded as per Table 10.5.5.32/3GPP TS 24.008 [12]:

LTE Cat-M1

```
0 0 0 0      1.28 s
0 0 0 1      2.56 s
0 0 1 0      3.84 s
0 0 1 1      5.12 s
0 1 0 0       6.4 s
0 1 0 1      7.68 s
0 1 1 0      8.96 s
0 1 1 1     10.24 s
1 0 0 0     11.52 s
1 0 0 1      12.8 s
1 0 1 0     14.08 s
1 0 1 1     15.36 s
1 1 0 0     16.64 s
1 1 0 1     17.92 s
1 1 1 0     19.20 s
1 1 1 1     20.48 s
```

NB-IoT

```
0 0 0 0      2.56 s
0 0 0 1      5.12 s
0 0 1 0      7.68 s
0 0 1 1     10.24 s
0 1 0 0      12.8 s
0 1 0 1     15.36 s
0 1 1 0     17.92 s
0 1 1 1     20.48 s
1 0 0 0     23.04 s
1 0 0 1      25.6 s
1 0 1 0     28.16 s
1 0 1 1     30.72 s
1 1 0 0     33.28 s
1 1 0 1     35.84 s
1 1 1 0      38.4 s
1 1 1 1     40.96 s
```

8.3.2 eDRX deep-sleep and paging only image

When the eDRX feature is supported by the network, it is possible for the module to further minimize its power consumptions by entering deep-sleep mode when not listening to paging in the PTW periods. This feature can be enabled as usual with AT+CPSMS=1 command, after having configured eDRX deep-sleep with AT+UPSMVER=8 command, which forces eDRX to be used standalone, disabling PSM requests to the network.

When the eDRX deep-sleep feature is used, power consumption can be further minimized by using a low power module FW called POI (Paging Only Image) loaded during periodic PTW periods. POI loading is enabled by default and can be disabled with AT+UPSMVER=8,0 command. When POI is loaded, the module is unresponsive until it changes status by itself, due to deep-sleep mode exit at periodic TAU, paging reception or early wake-up (which is effective only once the module has entered the deep-sleep state after the PTW period). Transitions between eDRX deep-sleep mode and POI can be monitored via the RXD or DSR UART lines, which become high during POI period, whereas the module status indication GPIO, V_INT RXD levels do not change with respect to eDRX deep-sleep state. Usage of POI in eDRX is notified with +UUPSMR: 1,2 URC when entering eDRX deep-sleep mode from normal operation.

8.3.3 Functional diagram of eDRX and PSM

For sake of clarity, Figure 5 illustrates the states transitions and device activity when both PSM and eDRX are active. Some configurable parameters are highlighted in the figure. In this case the negotiated eDRX cycle duration is TeDRX=1024 s. During the PTW, the module listens to paging continuously or discontinuously in case the network uses discontinuous reception. In below example the network uses discontinuous reception with a discontinuous reception cycle TDRX=2.56 s. It should be noticed that unlike PSM related timers, eDRX and DRX related ones start instant does not

depend on any previous RRC connection release. The negotiated T3324 and T3412 timers are also highlighted: eDRX is used during the T3324 active time.

1. The device is in PSM deep-sleep state, not responsive to AT commands nor paging messages. It has already registered at startup, negotiating PSM timers.
2. PSM is exited at early wake-up triggered by the host application or at T3412 timeout.
3. In case of an early wake-up the host application is expected to start a MO transmission. If a T3412 timeout occurs, the device sends a TAU keepalive message, performing a new PSM and eDRX negotiation. The device re-connects to the network.
4. Once the data or control packet transmission or reception is complete, the RRC connection is released by the network. The device enters the idle state and starts T3324 and T3412 timers.
5. While the T3324 timer is running, paging is listened to as per eDRX and DRX configuration.
6. PSM is entered after T3324 has elapsed. Operations continue as per point 1.

If after point 2 the device does not enter RRC connected state, the device will eventually re-enter PSM state as if it had not awakened from it.
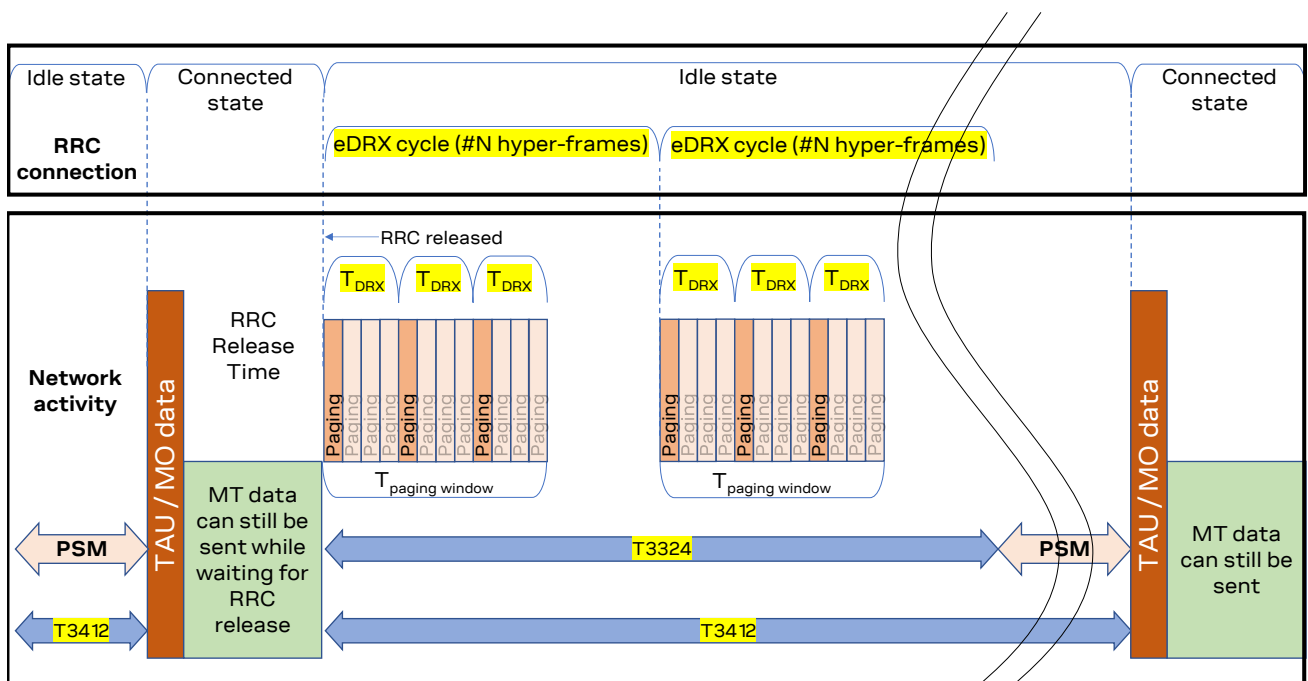
Figure 5: State transitions and module activity when both PSM and eDRX are enabled

9   Monitoring module status

9.1   Retrieve and interpret diagnostic information

It is recommended to track the module status in the host application. Such diagnostic information allows detection of specific scenarios and implementation of proper handling and countermeasures in the host application.

The module status can be returned by AT command responses and unsolicited result codes (URCs). Depending on the host application architecture, URCs, periodic polling, or both, can be used. URCs provide the most updated information and, in some cases, diagnostic information which is not available via polling. For AT commands that enable URCs, they might also return the same information when polled, as indicated below.

Some commands store the setting of the URC reporting in NVM, so they are referred to as persistent settings.

Some AT commands provide a choice on how to handle the URCs when the AT interface is busy; for all other AT commands, URC is issued at the return into command mode, as explained in SARA-R4 series AT command manual [2], in the "URCs presentation deferring" section.

URCs and AT command responses are presented with their generic syntax because parameters names are quite explanatory; for precise meaning, see the SARA-R4 series AT command manual [2].

9.1.1 Diagnostic information via URCs

Command	URC	Description	Can be polled
AT+CSCON=1	+CSCON: 1	Return the status of the RRC connection (idle or connected). Persistent setting.	Yes
AT+CREG=3	+CREG: <stat>[,[<lac>],[<ci>][,[<AcTStatus>][,<cause_type>,<reject_cause>]]]	Enable registration status URC for non-EPS services (for example, SMS) and reject cause in case of unavailability of such services.	Yes
AT+CEREG=5	+CEREG: <stat>[,[<tac>],[<ci>],[<AcT>][,[<cause_type>],[<reject_cause>][,[<Assigned_Active_Time>,[<Assigned_Periodic_TAU>]]]]]	Enable registration status URC for EPS services, reject cause in case of unavailability of such services and PSM related timers if granted by the network.	Yes
AT+CGEREP=2,1	+CGEV: NW PDN DEACT <cid>	Report all registration and PDN connectivity status events. The first parameter of the AT command is set to 2 indicate that URC will not be discarded in case the AT interface is busy.	No
AT+CTZR=1	+CTZV: <tz>	Enable reporting of changes in time zone. Usually, time zone information is provided by the network at LTE attach only.	No
AT+CMER=1,0,0,2,1	+CIEV: <descr>,<value>	Report variations in some indicators like roaming, SIM indication (provided that the feature is configured via +UGPIOC), signal level.	No
AT+CNMI=2,1	+CMTI: <mem>,<index>	Report the index in current selected memory (can be the factory-programmed setting ME or SIM, see +CPSM read command) where the mobile terminated SMS has been stored. The first parameter set to 2 indicates that URC are buffered in case of busy AT interface. The setting is volatile and shall be re-entered at every switch on or exit from PSM.	No
AT+USIMSTAT=7	+UUSIMSTAT: <state>	Report SIM initialization progress, SIM phonebook initialization progress, and SIM REFRESH events (each group of URCs can be singularly disabled). SIM Refresh URC might indicate the change of some operational parameters in the UICC card (for example, IMSI swap, SIM profile installation after remote SIM provisioning). The setting is persistent.	No
AT+UBIP=1	+UUBIP: <ev_cmd>,<val>	URC are raised when Open Channel, Close Channel, Send Data, Receive Data and Channel status events are issued by the SIM card towards the device to handle a SIM OTA session, for example for remote SIM provisioning. The embedded BIP client will cater for establishing the required socket and exchange data with the SIM OTA server. The setting is persistent.	No
AT+UFOTASTAT=1	+UFOTASTAT: <event>,<param1>[,<param2>]	Provide information on the progress and outcome of the Firmware download over the air via LwM2M (uFOTA). The setting is persistent.	No
AT+ULWM2MSTAT=1	+ULWM2MSTAT: <event>,<param1>[,<param2>]	Enable URC to report the activity of the embedded LwM2M client. The setting is persistent.	No

Command	URC	Description	Can be polled
AT+CEINFO=1	+CEINFO: <reporting>,<CE_enabled>,<UE_state>,<downlink_repetition_factor>,<uplink_repetition_factor>,<RSRP_value>,<CINR>	Volatile setting, it reports variation of the Coverage extension mode and related transmission parameters (for example, repetitions schemes to be used) detected by the device or assigned by the network.	Yes
AT+CEDRXS=1	+CEDRXP: <AcT_type>[,<Requested_eDRX_cycle>[,<Assigned_eDRX_cycle>[,<Assigned_paging_time_window>]]]	If eDRX is used by the host application, the URC can report changes in eDRX settings imposed by the network in different areas or times. The setting is persistent.	Yes

☞ Always consider to apply the +CGEREP AT command with <mode> equal 2, for example AT+CGEREP=2, in order to avoid to lose URCs when the AT interface is busy in executing some other AT commands.

9.1.2 Diagnostic information via polling

Command	Response (omitting OK)	Description	Suggested usage
ATI ATI9	SARA-R422M8S-00B-00 00.06,A00.00	Return the model and FW identification, useful for tracking purposes.	Module initialization
AT+CGSN	355438110017558	Return the IMEI.	Module initialization
AT+CIMI AT+CCID	001010123456789 +CCID: 89860000502000180722	Return the SIM identities for tracking purposes. They can change after a SIM refresh event that can be reported by +UUSIMSTAT URC.	Module initialization
AT+UBANDMASK?	+UBANDMASK: 0,185079967,2,1,134748319,1048642,2,2621824	Return band mask selection.	Module initialization
AT+UMNOPROF?	+UMNOPROF: 90	Return MNO profile set.	Module initialization
AT+UCGED?	+UCGED: 2 6,<svc>,<MCC>,<MNC><EARFCN>,<Lband>,<ul_BW>,<dl_BW>,<TAC>,<LcellId>,<P-CID>,<mTmsi>,<mmeGrId>,<mmeCode>,<RSRP>,<RSRQ>,<Lsinr>,<Lrc>,<RI>,<CQI>,<avg_rsrp>,<totalPuschPwr>,<avgPucchPwr>,<drx>,<l2w>,<volte_mode>[,<meas_gap>,<tti_bundling>	Return several cell parameters as measured by the module or provided by the network. Some values like CQI and signal indicators are periodically refreshed in the module on a 0.5 s base, so the application should average them.	Low periodicity
AT+CESQ?	+CESQ:,,,,<rsrq>,<rsrp>	Return signal quality and level, and it is more precise than +CSQ. It is subjected to transitions due to local reset of values at changes in RRC state (idle, connected) so the host application should average the values.	Periodically (for example, every 50 to 10 s)

Command	Response (omitting OK)	Description	Suggested usage
AT+COPS?	+COPS: <mode>[,<format>,<oper>[,<AcT>]]	It returns the current registered PLMN in the configured format, RAT is fixed to 7 (LTE, Cat-M1).	Periodically (30 s) and when detecting problems
AT+CGDCONT?	+CGDCONT: <cid>,<PDP_type>,<APN>,<PDP_addr>,<d_comp>,<h_comp>[,<IPv4AddrAlloc>,<request_type>,<P-CSCF_discovery>,<IM_CN_Signalling_Flag_Ind>[,<NSLPI>[,<secure_PCO>[,<IPv4_MTU_discovery>[,<Local_Addr_Ind>]]]]]	It returns the active and defined EPS bearers with the APN used and the IP type and addresses.	Periodically (30 s) and when detecting problems
AT+CPOL?	+CPOL: <index1>,<format>,<oper1>[,<GSM_AcT1>,<GSM_Compact_AcT1>,<UTRAN_AcT1>[,<E-UTRAN_AcT>]]	It returns the high priority PLMN list, which might change at SIM refresh.	Module initialization and SIM refresh, only in debug/test mode
AT+CEDRXRDP	+CEDRXRDP: <AcT_type>[,<Requested_eDRX_cycle>,<Assigned_eDRX_cycle_value>,<Assigned_paging_time_window>]	It returns the current eDRX parameters assigned by the mobile network.	If eDRX is used, the host should monitor CTS line to avoid waking up the module during eDRX/sleep periods
AT+CPSMS?	+CPSMS: <mode>,[<Requested_Periodic_RAU>],[<Requested_GPRS_READY_timer>],[<Requested_Periodic_TAU>],[<Requested_Active_Time>]	It returns the PSM settings as required to the network. As setting is persistent, if the network does not grant PSM, the module will propose the PSM timers at every attach and registration attempt.	Module initialization
AT+UCPSMS?	+UCPSMS: <mode>,[<Assigned_Periodic_RAU>],[<Assigned_GPRS_READY_timer>],[<Assigned_Periodic_TAU>],[<Assigned_Active_Time>],[<Assigned_Periodic_TAU_Format_Type>]	It returns the PSM settings as assigned by the network. If PSM timers are not reported by +CEREG, this command can be periodically polled. Periodic TAU timer is also reported.	At change of registration information (as reported by +CEREG)

9.2 Full-stack watchdog: how to react to unexpected conditions

The application shall properly handle communication or connectivity problems that can arise when using the module in the cellular mobile environment.

When a problem at a specific level is encountered, the countermeasure for that level should be tried and, if that does not resolve the issue, then proceed with the solutions for the lower levels. Table 11 shows a full-stack watchdog for monitoring SARA-R4 series modules.

Level	Problem	Countermeasure	AT commands / actions	Notes
Socket/dial-up	Cannot send/receive data	Close and re-open socket	`AT+USOCL=<socket_id>` `AT+USOCR=<protocol>` `AT+USOCO=…`	
		Disconnect and re-connect dial-up	Send +++ / Move DTR `ATD*99***<cid>#`	
IP/PDP	Cannot get an IP address; cannot establish dial-up	Detach/re-attach	`AT+CFUN=0` `AT+CFUN=1`	Consider possible restrictions to multiple <cid>s active for APN. If IPv6-only PDN is set in Verizon Wireless MNO setting, detach/deactivation may be caused by failing IPv6 acquire by SLAAC. The retry is managed automatically based on VZW DR logic. Automatic deactivation does not apply if UL data is disabled via +UMNOPROF: 9,0.
		Deactivate/re-activate context (<cid> != 1)	`AT+CGACT=0,<cid>` `AT+CGACT=1,<cid>`	
Network registration	Cannot register	Detach/re-attach	`AT+CFUN=0` `AT+CFUN=1`	AT+CFUN=0/1 has to be preferred for registration cycles. Moreover AT+CFUN=0/1 is faster than AT+COPS=2/0.
RF	Cannot register	Disable/re-enable RF functionality	`AT+CFUN=0` `AT+CFUN=1`	AT+CFUN=4 is NVM persistent, better to use AT+CFUN=0.
Module FW	Cannot register	Soft reset	`AT+CFUN=15`	
AT interface	No response from module	HW switch off	GPIO power control	See the SARA-R4 series system integration manual [3] for details and alternatives.

Table 11: Full-stack watchdog for SARA-R4 series modules

10 Testing

10.1 OEM production testing

The `+UTEST` AT command is used for non-signaling testing to verify proper assembly of the module and the involved parts in the OEM production line. It is intended for use by the manufacturer of the host device integrating the module.

☞ The `+UTEST` AT command is not expected to be used for cellular RF performance measurements neither for certification purposes.

⚠ u-blox assumes no responsibility for inappropriate use of the `+UTEST` command.

⚠ The use of this command shall be restricted to controlled (shielded chamber/box) environments and for test purposes only.

In particular, the `+UTEST` AT command allows to check all the RF parts and digital pins, that is, proper soldering of the ANT pad and related parts along the RF path, and GPIO functionality testing. The usage of this command should be restricted to controlled RF environments, such as shielded chamber/box, and shall be confined to validation and production tests.

The command requires entrance into test mode, so full functionality shall be restored after its usage.

It is suggested to test the module using the final MNO profile (if different from `+UMNOPROF: 1`, unless the final SIM card is used) and configuration (LwM2M, security, APN, etc.) and in all bands it will be operational (with the `+UBANDMASK` AT command).

If possible, it is suggested to use test SIM cards during production tests, possibly the same SIM card used during the device validation. If a test SIM card is not available, and if the production tests are performed in signaling mode on a network simulator, make sure to disable authentication and integrity checks on the tester side (by proper setting) and on the module (by using the `AT+UDCONF=81,0` command, see SARA-R4 series AT commands manual [2]) and consider that LwM2M and security features might trigger uplink data transmission. Also consider that, at new SIM card detection, LwM2M will need about 20 s to populate its database and being ready to operate: this can be done in the production phase or once the device is deployed in the field.

10.1.1 Entering and exiting the RF non-signaling mode

Enable the non-signaling mode to start using `+UTEST`; to do so issue `AT+UTEST=1` command.

☞ Deregister the module from the network before enabling non-signaling mode. Issue the `AT+COPS=2` command to deregister from the network, otherwise the "`+CME ERROR: operation not allowed`" or "`+CME ERROR: 3`" (depending on the `+CMEE` AT command setting) will be reported.

Table 12 shows an example of entering non-signaling mode.

Command	Response	Description
`AT+UTEST?`	`+UTEST: 0` `OK`	Check the device is in signaling mode.
`AT+COPS=2`	`OK`	Deregister the module from the network.
`AT+UTEST=1`	`OK`	Enter the non-signaling mode.
`AT+UTEST?`	`+UTEST: 1` `OK`	Check the +UTEST AT command is in non-signaling mode.
`AT+UTEST=3,123130,23,,,5000`	`+UTEST: 123130,23,5,1,5000` `OK`	Example 1: TX test executed on B12 TX, Ch. 123130, 23 dBm, TX output for 5 s.

Command	Response	Description
`AT+UTEST=2,105060,5000`	`+UTEST: 105060,5000,0,-21,-20,-19` `OK`	Example 2: RX test executed on B12 TX, Ch. 105060, RX measurement on for 5 s. The signal input to the receiver is reported at -20 dBm.

Table 12: Entering non-signaling mode with +UTEST

After the desired tests have been executed, perform this to return to normal operating mode:

- Send `AT+UTEST=0`. Make sure to restore the full operational `+CFUN` mode via `AT+CFUN=0/1` cycle.

10.1.2 Cellular RF functional test

As mentioned before, OEM manufacturers need only to verify proper assembly of the module in the OEM production line. This can be done by performing a simple RF functional test with basic instruments such as a spectrum analyzer (or an RF power meter), and optionally a signal generator, with the assistance of the `+UTEST` AT command over the AT command user interface.

In test mode, the module switches off the protocol stack for performing single tests that could not be performed during signaling. The `+UTEST` AT command provides a simple interface to set the module to RX or TX test modes ignoring the LTE signaling protocol. The command can set the module into:

- Transmitting mode in a specified channel and power level in all supported bands.
- Receiving mode in a specified channel to return the measured power level in all supported bands.

The minimum recommended RF verification in production consists in forcing the module to transmit in a supported frequency with the `+UTEST` AT command, and then checking that some power is emitted from the antenna system using any suitable power detector, power meter or equivalent equipment. For a detailed explanation of the hardware setup, see the SARA-R4 series system integration manual [3].

Table 13 and Table 14 report examples of RF tests using `+UTEST`, both in transmitting and in receiving modes.

Command	Response	Description
`AT+COPS=2`	`OK`	Deregister the module from the network.
`AT+UTEST?`	`+UTEST: 0` `OK`	Check the device is in signaling mode.
`AT+UTEST=1`	`OK`	Enter the non-signaling mode.
`AT+CFUN=15`	`OK`	Perform a reset.
`AT+UTEST=1`	`OK`	Enter the non-signaling mode again.
`AT+UTEST?`	`+UTEST: 1` `OK`	Check the module is in non-signaling mode.
`AT+CFUN?`	`+CFUN: 5` `OK`	Check +CFUN AT command is set to 5 to ensure the module is in test mode. The device is now ready for either TX, RX non-signaling tests.
`AT+UTEST=3,119575,-30,,,1000`	`+UTEST: 119575,-30,5,1,1000` `OK`	The module transmits at channel 19575 (frequency 1747.50 MHz LTE band 3) for 1 s, after which the "OK" final result code is returned. After the "OK" final result code, another +UTEST command can be sent.

Table 13: example of +UTEST RF Tx testing

For SARA-R4 series modules the RF output resulting from the `AT+UTEST=3` command is a QPSK-modulated continuous signal with a bandwidth of 360 kHz (2 resource blocks).

Command	Response	Description
AT+COPS=2	OK	Deregister the module from the network.
AT+UTEST=1	OK	Enter the non-signaling mode again.
AT+UTEST?	+UTEST: 1 OK	Check the module is in non-signaling mode.
AT+CFUN?	+CFUN: 5 OK	Check +CFUN AT command is set to 5 to ensure the module is in test mode. The device is now ready for either TX, RX non-signaling tests.
AT+UTEST=2,101575,1500	+UTEST: 101575,1500,0,-70,-70,-70 OK	The module measures the receiver power level for 1.5 s at channel 1575 (frequency 1842.50 MHz LTE band 3). After the time interval, the information text response contains: the channel number, the time interval and the minimum, average, maximum power levels.

Table 14: Example of +UTEST RF Rx testing

For any module (factory brand-new or not) when exiting the non-signaling mode to get back into the signaling mode, it is important to check that the device has properly been restored to signaling mode. This requires a check between the +UTEST and +CFUN state to see if they are in agreement.

Example of checking module is properly in signaling mode after it exits +UTEST non-signaling mode:

Command	Response	Description
AT+UTEST?	+UTEST: 0 OK	The device is in normal mode.
AT+CFUN?	+CFUN: 5 OK	The device is not completely in non-signaling mode because +CFUN reports that it is in test mode. Below is the sequence to correct this.
AT+CFUN=0	OK	Set the MT to minimum functionality.
AT+CFUN=1	OK	Sets the MT to full functionality.
AT+CFUN?	+CFUN: 1 OK	The device is now set to full functionality.
AT+UTEST?	+UTEST: 0 OK	The device is in signaling mode. Both the +CFUN and +UTEST AT commands agree that the device is in signaling mode.

10.1.3 UTEST RX and TX non-signaling test sequence

☞ It is recommended to perform all RX UTEST grouped sequentially together, separate from the TX UTESTs test grouped sequentially together. This may help avoid measurement glitches.

A glitch is defined as a measurement output of an expected value, but reports a value with a significant differential. Example: if the module were instructed to transmit 20 dBm, but the device actually transmits 0 dBm, and there is no RF connectivity hardware at fault, then this is likely a glitch.

If a glitch should be encountered then a reset (AT+CFUN=15) and re-entry back into UTEST non-signaling mode is required to clear the glitch.

A measurement glitch does not occur randomly; it can happen through a combination of TX and RX measurements and is reproducible. Therefore, if a glitch is encountered in the development of the +UTEST sequence, then it will not unexpectedly change the behavior with the same sequence repeated.

☞ Any +UTEST sequence should be verified with measurements before deploying into production.

Example of grouping TX and RX tests in non-signaling RF mode:

Command	Response	Description
AT+UTEST=3,123060,23,,,5000	+UTEST: 123060,23,5,1,5000 OK	TX test on B12, Ch. 123060, 23 dBm, 5 s on.
AT+UTEST=3,123095,23,,,5000	+UTEST: 123095,23,5,1,5000 OK	TX test on B12, Ch. 123095, 23 dBm, 5 s on.
AT+UTEST=3,120000,23,,,1000	+UTEST: 120000,23,5,1,1000 OK	TX test on B4, Ch. 120000, 23 dBm, 1 s on.
AT+UTEST=3,120100,23,,,1000	+UTEST: 120100,23,5,1,1000 OK	TX test on B4, Ch. 120100, 23 dBm, 1 s on.
AT+UTEST=2,105020,2000	+UTEST: 105020,2000,0,-20,-20,-19 OK	RX test on B12, Ch. 105020, 23 dBm, 2 s on[2].
AT+UTEST=2,105070,2000	+UTEST: 105070,2000,0,-21,-20,-20 OK	RX test on B12, Ch. 105070, 23 dBm, 2 s on[1].
AT+UTEST=2,102000,2000	+UTEST: 102000,2000,0,-21,-20,-20 OK	RX test on B4, Ch. 102000, 23 dBm, 2 s on[1].
AT+UTEST=2,102100,2000	+UTEST: 102350,2000,0,-21,-20,-20 OK	RX test on B4, Ch. 102350, 23 dBm, 2 s on[1].

10.1.4 UTEST RF TX non-signaling continuous mode

For TX non-signaling mode, avoid using continuous mode if possible due to the internal mode TX flag not getting cleared when transitioning to the next non-signaling test.

If the continuous mode is used, then issue a subsequent non-continuous mode of the same frequency, channel, and power output to clear an internal flag.

Example of clearing an internal flag if the continuous mode is used for RF TX non-signaling mode:

Command	Response	Description
AT+UTEST=3,123060,23,,,0	OK	Turn on the continuous TX in B12, Ch. 123060, 23 dBm.
AT+UTEST=3,123060,23,,,1000	+UTEST: 123060,23,5,1,1000 OK	Turn on TX for 1 s in B12, Ch. 123060, 23 dBm This will clear the internal TX flag set by continuous mode.

10.1.5 Digital test

This test mode can be used during OEM production testing to check the correct behavior of the module's digital pins and detect possible soldering or functional problems.

The +UTEST AT command can be used to configure a specific group of pins as:

- Digital input: once configured, it is possible to apply a voltage level to the pin.
- Digital output: the pin can be used to output a digital "high" or "low" voltage level.

Pins enabled for digital testing can be considered as generic digital input / output pins; it is possible to configure a pin as a digital output with "high" logic level and then verify the voltage level present at the pin. Conversely, it is possible to apply a "high" or "low" logic level on a pin set as a digital input, and then check if the module can correctly measure the voltage level applied.

Table 15 reports number and type of pins available for digital testing via the +UTEST AT command. For a detailed description of the input / output levels characteristics of the pins, see the SARA-R4 series data sheet [1].

---

[2] Use 100 kHz offset from center frequency of RF input signal. For example, to test EARFCN=2525 of LTE B5, corresponding to 881.50 MHz, set the RF frequency of the generator to 881.50 + 0.1 = 881.6 MHz. Modulation setting is not required.

Pin no	Name	Interface
6	DSR	UART
7	RI	
8	DCD	
9	DTR	
10	RTS	
11	CTS	
16	GPIO1	GPIO
19	GPIO6	
23	GPIO2	
24	GPIO3	
25	GPIO5	
26	SDA	DDC
27	SCL	
34	I2S_WA	Audio
35	I2S_TXD	
36	I2S_CLK	
37	I2S_RXD	
42	GPIO5	GPIO

Table 15: List of pins available for +UTEST digital testing

Below is an example of configuring GPIO 1 as output and set to high.

Command	Response	Description
AT+CMME=2	OK	Configure the formatting of the error result code by means of the +CMEE AT command.
AT+COPS=2	OK	Deregister the module from the network.
AT+UTEST=1	OK	The module enters the test mode.
AT+UTEST=10,1	(pin description returned) OK	Gets the pin information.
AT+UTEST=10,2,"000000000000 000000008000"	OK	Put the module in interface initialized state; the command saves the pins status to restore it at the end of the test. Pins enabled for testing: GPIO1 pin 16 Where hex: 0000 0000 0000 0000 0000 8000
AT+UTEST=10,3,"000000000000 000000000000"	OK	GPIO1 is configured for output where the bits for pin 16 are set low Where hex: 0000 0000 0000 0000 0000 0000
AT+UTEST=10,4,"000000000000 000000008000"	OK	GPIO1 is set to high for pin 16 Where hex: 0000 0000 0000 0000 0000 8000
AT+UTEST=10,5		Configurations made by the AT+UTEST=10,2; AT+UTEST=10,3 and AT+UTEST=10,4 commands are executed.
AT+UTEST=10,6	0000000000000000000008000 OK	Logic digital value measured at modules pins for GPIO1, and "high" level detected.

Below is an example of configuring RTS and CTS as output and set to high. This example can only be done through the USB interface.

Command	Response	Description
AT+CMME=2	OK	Configure the formatting of the error result code.
AT+COPS=2	OK	Deregister the module from the network.
AT+UTEST=1	OK	The module enters the test mode.

Command	Response	Description
`AT+UTEST=10,1`	`(pin description returned)` `OK`	Gets the pin information.
`AT+UTEST=10,2,"000000000000` `000000000600"`	`OK`	The command puts the module in Interface initialized state; the command saves the pins status to restore it at the end of the test. Pins enabled for testing: RTS pin 10, CTS pin 11 Where hex: 0000 0000 0000 0000 0000 0600
`AT+UTEST=10,3,"000000000000` `000000000000"`	`OK`	RTS and CTS are configured for output where the bits for the pins 10,11 are set low Where hex: 0000 0000 0000 0000 0000 0000
`AT+UTEST=10,4,"000000000000` `000000000600"`	`OK`	RTS and CTS is set to high for pin 10, 11 Where hex: 0000 0000 0000 0000 0000 8000
`AT+UTEST=10,5`		Configurations made by the AT+UTEST=10,2; AT+UTEST=10,3 and AT+UTEST=10,4 commands are executed.
`AT+UTEST=10,6`	`000000000000000000000600` `OK`	Logic digital value measured at modules pins for GPIO1, and "high" level detected.

- When a module is programmed to enter the end user test mode, the `+CFUN: 5` URC will be reported if the module is in non-signaling mode, and it can be used as an indication the module does not exit properly the non-signaling mode.

☞ If the +UGPIOC, +UGPIOR, and +UGPIOW AT commands are used in the same power-up session, then apply these commands before applying the AT+UTEST=10 command. This will allow the AT+UTEST=10 command to interact with the pins effectively, and not have conflicting control with the other commands.

10.2 Network simulators testing

When testing with network simulators, such as a CMW500 from Rohde & Schwarz as one example among many, the simulator may not be configured to release the RRC connection when there is an idle period.

By means of the +UMACQOSTMR AT command, this timer may need to be disabled to allow certain measurements. RF sensitivity measurements, for example, expect the RRC connection to remain in the connected state. If this MAC QoS timer is not disabled, then after the timer expires, it will release the RRC connection with the simulator and may interrupt the measurement.

Here below it is reported an example of checking for the MAC QoS timer value and setting it.

Command	Response	Description
`AT+UMACQOSTMR?`	`+UMACQOSTMR: 90,120` `OK`	Check if MAC QoS timer is enabled by reading it. In this example, it is enabled for LTE Cat M1 with 35 s, while it is enabled for NB-IoT with 120 s.
`AT+UMACQOSTMR=0,0`	`OK`	Disabled MAC QoS timer for both LTE Cat M1 and NB-IoT with 0 value set.
`AT+CFUN=15`	`OK`	Reset the device for new value to disable MAC QoS timer.
`AT+UMACQOSTMR?`	`+UMACQOSTMR: 0,0` `OK`	Confirm MAC QoS timer is disabled, which in this example it is reflected as disabled with "0" value for both LTE Cat M1 and NB-IoT.

Other factors to consider with using a test simulator are:

- the need for utilizing a dedicated test SIM: for more details, see section 11.1;
- in Radio Bearer (RB) Test Mode, the +CGDCONT test command does not show any APN and any IP address after getting a valid registration on the simulated network.

11 SIM

11.1 Chip SIM

For devices utilizing a physically soldered down chip SIM, consider what network or networks the device will connect to. More specifically, beyond the obvious intended end network(s) the device will deploy on, keep in mind the need to connect with a test network or base station simulator call-boxes, which may require a specific UICC profile to connect to. Anticipate such needs and be prepared to be able to obtain and configure a profile to connect to such networks or simulators.

Alternatively, here below some other possible ways to proceed for testing purposes:

- Configure a device(s) with a SIM card holder for physical removable SIM for such engineering or pre-production activities.
- Make sure to disable authentication and integrity checks on the tester side (by proper setting) and on the module (by using the `AT+UDCONF=81,0` AT command, see SARA-R4 series AT commands manual [2]).

12 SMS

12.1 Preferred message storage

The factory-programmed value for SARA-R4 series modules is "ME" for the three memory parameters <mem1>, <mem2> and <mem3>. The setting can be set or read by the +CPMS AT command.

This is an example regarding the configuration of the +CPMS storage parameter for all memory parameters to the same value.

Command	Response	Description
AT+CPMS="ME","ME","ME"	+CPMS: 0,23,0,23,0,23 OK	Set all three memory storage parameters to "ME" memory storage.
AT+CPMS?	+CPMS: "ME",0,23,"ME",0,23,"ME",0,23 OK	Read the storage setting back.

For more details on the +CPMS AT command, see SARA-R4 series AT commands manual [2].

12.2 SMS handling and access technology

All SARA-R4 MNO profiles use Combined Attach (CS & PS); if successful, both data and SMS services are allowed. If LTE attach is successful for EPS only services, still SMS can be supported (the so called "SMS only" case). If LTE attach is not successful for SMS, the module can try registration on a different RAT (e.g. 2G).

Accordingly the SMS support could be related to the selected access technology.

In particular, if AT+URAT=8 is applied, the attach becomes "EPS only" (with "SMS only" additional update type included). In this case, even if SMS services are accepted, the +CREG read command and URC would report that it is not registered for CS services.

Since it can happen that SMS services are not supported in NB-IoT, in AT+URAT=8 there is no means to understand this other trying to send out an SMS. In addition, due to the fact that the network is not including SMS only flag in the Attach accept, the module will repeat TAU every 10 s approximately, with a consequent high power consumption. Summarizing:

1. In mono-RAT (NB-IoT), i.e. AT+URAT=8, registered on a network without SMS support:

   o Tracking Area Update (TAU) procedures every 10 s for maximum 5 times every 12 minutes (around 25 times per hour);
   o pay attention to power consumption;

2. In multi-RAT (NB-IoT plus LTE Cat M1 and/or 2G), e.g. AT+URAT=7,8,9, registered on a network without SMS support:

   o no TAU procedures every 10 s;
   o longer network scans (in any case the NB-IoT is the RAT with longest scans);
   o this configuration could be considered as a possible trade-off;

3. In multi-RAT (NB-IoT plus LTE Cat M1 and/or 2G), e.g. AT+URAT=7,8,9 registered on a network with SMS support:

   o +CREG indication is reliable in 2G RAT;
   o +CREG indication is not reliable in LTE Cat M1/NB-IoT, accordingly try to send a SMS;
   o +CSCON indication reports information about the radio connection status.

In conclusion the possibility to work in a multi-RAT configuration could be recommended and considered as a possible workaround referring the scenarios described in the above points 1 and 2.

13 EFS backup & restore

Due to the nature of Flash memory, the Embedded File System (EFS) may incur memory corruption if the safe & graceful shutdown procedure outlined in the SARA-R4 series system integration manual [3] is not followed. It is possible that memory corruption may result in the device being inoperable or impact specific device data information.

For a fatal memory corruption, the EFS backup & restore feature allows the module to autonomously restore the EFS using the last EFS backup stored on the module itself.

Backup of device's unique parameters (like for example RF calibration data, IMEI, etc.) is performed at the u-blox factory and is stored on the module as the first backup copy for the device. The host application has the option to make subsequent backups to supersede the previous backup copy. If an EFS corruption is detected, then the restore is triggered autonomously at the device boot-up process to restore the device with the single backup copy stored on the device.

Backup & Restore is a unique feature that may extend the lifetime of the modules in the field.

☞ It is critical that the host application follows the proper safe & graceful shutdown procedure outlined in the SARA-R4 series system integration manual [3]. Backup & Restore feature is intended only as an additional backup mechanism if, on the potential rare occasion, the host application shutdown is not conforming to the graceful power down guidelines.

13.1 Description

There are two parts to the EFS backup & restore feature for SARA-R4 series modules.

First, the Restore function allows the modules to automatically recover from a fatal file system corruption if it should detect such a corruption from previous improper shutdown at the next module boot-up. If the corruption is non-fatal, where the module can boot up, then the host can manually trigger a restore.

These non-fatal corruption types are considered:

* Lost of IMEI
* MNO profiles lost or duplicated
* Device goes into the non-signaling mode (for more details, see +UTEST AT command)

☞ A restore should be host triggered only in one of the above conditions.

The second part of this feature is optional for a device that comes with this feature from the factory, where the host can perform a backup of the file system to supersede the previous or original backup done during the module production. This will allow the latest user values in the file system to be captured in the backup copy. The procedure could include security data, e.g. certificates.

☞ Only personalization data for security, calibrations and unique data will be restored. Instead, user files, parameters and profiles will be set to default, i.e. they will not be considered by the backup and restore process.

13.1.1 EFS backup

The EFS backup can be initiated with the `+UBKUPDATA` AT command and will automatically trigger a backup process upon receiving the command. After this procedure is completed, the device will store status information that can be queried with an AT command. After the backup completion, no further action is required.

The host can issue backup on an infrequent & rare basis that justifies for such a need to perform a backup. This could be when some important and significant information in the file system has changed or been added via AT commands, e.g. regarding the personalization data for security. One likely point of needing a backup is after the host application factory initial "production", which may include the module configuration to a specific use case requirement related to the security functionalities. The backup command can also provide some information about the last backup.

The command's query response contains the number of backups and restores for each file system.

☞ There are not multiple backup "versions" stored; only a single copy of the latest backup is kept.

☞ To avoid excessive flash wear, the backup should be performed on a limited basis such as after host application production and initialization.

☞ It can take up to 15 s for a backup to execute.

To detect when the backup function is complete, and the AT interface is available here is the following option:

- Wait for **+UUBKUPDATA** URC
  - Example for backup successful: **+UUBKUPDATA: 1,1**

13.1.2 EFS restore

When an automatic restore is triggered, the device will immediately reset/restore the file system (this may interrupt any currently running processes). The device will then reset, and store status information that can be queried with an AT command. After the restore procedure is completed, no further action is required, although some settings may need to be restored manually by the user, if they were modified since the last backup.

If the restore process is interrupted (e.g. through power pull), the process will start from the beginning again at the next module boot-up.

There is no available indication to the host processor that a restore is taking place during boot-up; it would just appear as if boot-up is taking longer than typical. If a restore should take place, then the host processor would need to allow more time for the device to handle the restore, until the AT interface is made available.

☞ It can take up to 15 s for a restore to execute. This time includes the boot-up time.

The host can detect when a restore has taken place by a URC notification. Example: the **+UUBKUPDATA: 2,1** URC indicates the restore has taken place and is successful.

A manual restore can be triggered when one of the following conditions is detected by the host:

- Lost of IMEI, which can be checked and detected with the `+CGSN` AT command, where:
  - `+CSGN` would return the "+CME ERROR: memory failure" error result code
- MNO profiles lost or duplicated, which can be checked and detected with `+UMNOPROF` AT command

- The device goes into the non-signaling mode and is unable to exit with `AT+UTEST=0` and `+CFUN` cannot change its state from a value of 5. This non-signaling state can be checked and detected with the `+CFUN` read command, where the device would return a value of 5.

Restore is only intended for the above situations.

Example on using `+CGSN AT` command to detect lost IMEI

Command	Response	Description
`AT+CGSN`	`+CME ERROR: memory failure`	Error result code indicates lost IMEI using +CGSN AT command.

With the possibility of a restore event, to detect when the module boot-up is complete and AT interface is available here are following options:

- Loop AT until the "OK" final result code is issued
  - Example: send AT every one second until the OK final result code is received
- Enable and monitor the GPIO pin with "Module status indication" functionality via the `+UGPIOC` AT command
- Enable and monitor the greeting message via the `+CGST` AT command

13.1.3 Creating backup after flashing FW update with delta package

If a FW build with the Backup & Restore feature is being updated via FOTA / uFOTA with a delta package, then after the successful update a restore is triggered autonomously by the module itself.

13.1.4 EasyFlash, backup and SMS storage

If a FW build with the Backup & Restore feature is being flashed onto a module via EasyFlash, after a successful FW update when the device boots up, then the host is required to:

- define a new EFS backup through the `+UBKUPDATA` AT command;
- set the preferred SMS message storage with `+CPMS` AT command just once after flashing. This step is required if the host application should use SMS. If it does not intend to use SMS, then this step can be ignored. Even if the host intends to use the `+CPMS` factory-programmed setting, the storage setting still needs to be set.

14 Restore factory configuration

During operation with the module, different files may be stored in the module's file system. Similarly, the NVM is populated with user configuration as well as auxiliary information stored by the module to optimize its operations (e.g. information on the cellular environment).

☞ Profiles can be restored with `ATZ` command.

☞ AT commands factory-programmed values stored in NVM and profiles are listed in appendix B.2 of SARA-R4 series AT commands manual [2].

The host application can restore the module factory configuration via the `+UFACTORY` AT command (see the SARA-R4 series AT commands manual [2]); this can be required to recover from an unexpected behavior and restart the module in a controlled configuration, or during the MNO certifications, where the device is tested in various simulated scenarios and the auxiliary information or previous user settings can affect the tests outcome.

Restoring the factory configuration of the module is a 2-step process:

1. Set the type of restore to perform, using the `+UFACTORY` AT command. FS and/or NVM can be restored.
2. Reboot the module.

The `+UFACTORY` AT command writes a flag in NVM and does not perform any restoring action. This flag is then read **at the next reboot,** when the +UFACTORY corresponding action is executed. Therefore it is possible to cancel the +UFACTORY action by issuing the `AT+UFACTORY=0,0` command **before the reboot**.

Table 16 shows some examples.

Command	Response	Description
Delete all user files previously saved with USER flag in the file system		
AT+UFACTORY=1,0	OK	Set +UFACTORY to delete all user files previously stored with USER flag in the file system. No restore is performed so far.
AT+UFACTORY?	+UFACTORY: 1,0 OK	Check the restore action currently set.
AT+CFUN=16	OK	Reboot the module. At next reboot, the restore action previously set is applied.
Delete all modem profiles in NVM		
AT+UFACTORY=0,1	OK	Set +UFACTORY to delete all modem profiles, in detail native modem profiles are reset, while added modem profiles are deleted. No restore is performed so far.
AT+UFACTORY?	+UFACTORY: 0,1 OK	Check the restore action currently set.
AT+CFUN=16	OK	Reboot the module. At next reboot, modem profiles are reverted to the factory programmed values.
Restore UART and UPSV settings to default in NVM		
AT+UFACTORY=0,2	OK	Set +UFACTORY to restore UART and +UPSV settings to default in NVM. No restore is performed so far.
AT+UFACTORY?	+UFACTORY: 0,2 OK	Check the restore action currently set.

Command	Response	Description
AT+CFUN=16	OK	Reboot the module. At next reboot, UART and +UPSV settings are reverted to the factory programmed values.
Cancel a delete operation (before reboot)		
AT+UFACTORY=1,0	OK	Set a +UFACTORY action.
AT+UFACTORY?	+UFACTORY: 1,0 OK	Check the action currently set. At the moment, a delete user files procedure is requested and will be applied at next reboot.
AT+UFACTORY=0,0	OK	Cancel any delete action.
AT+UFACTORY?	+UFACTORY: 0,0 OK	No delete action will be applied at next reboot.

Table 16: +UFACTORY AT command usage examples

☞ After having issued a +UFACTORY AT command with <nvm_op>=1, it is required a second reboot to make the module again ready to properly accept and store new settings to NVM.

15 Specialized application notes by topic

15.1 Multiplexer

See the Mux implementation in cellular modules application note [8].

15.2 IP based applications

See the Internet applications development guide application note [5].

15.3 Security suite

See the Security suite application note [6].

15.4 Secure communication

See the Internet applications development guide application note [5].

15.5 GNSS

See the SARA-R4 / SARA-R5 series GNSS implementation application note [7].

15.6 LwM2M

See the LwM2M objects and commands application note [9].

15.7 AWS IoT core

See the SARA-R5 SARA-R422 AWS IoT Core application note [10].

15.8 FW update

See the SARA-R4 FW update application note [4].

16 Migration guide from SARA-R410M / SARA-R412M and hints

Below is a list of software changes between SARA-R410M / SARA-R412M and SARA-R422 / SARA-R422S / SARA-R422M8S modules with a brief description, which could help in migrating a host application between the two modules. For detailed explanation of the AT commands mentioned, see the SARA-R4 series AT commands manual [2].

Command or feature	SARA-R422 / SARA-R422S / SARA-R422M8S	SARA-R412M-02B-03	SARA-R410M-63B / SARA-R410M-73B / SARA-R410M-83B	SARA-R410M-02B-03
RATs	• 3GPP Rel. 14 LTE Cat M1 • NB2 • EGPRS	• 3GPP Rel. 13 LTE Cat M1 • NB1 • EGPRS	• 3GPP Rel. 13 LTE Cat M1 • NB1 (not supported by "63B" and "73B" product versions)	• 3GPP Rel. 13 LTE Cat M1 • NB1
Connected Mode Mobility (CMM)	Handover Intra-band & Inter-band	n.a.	Handover Intra-band	n.a.
USB enumeration	• HS-USB Diagnostics 90B2	• HS-USB Modem 90B2 • HS-USB Diagnostics 90B2 • HS-USB WWAN Adapter 90B2	• HS-USB Modem 90B2 • HS-USB Diagnostics 90B2 • HS-USB WWAN Adapter 90B2	• HS-USB Modem 90B2 • HS-USB Diagnostics 90B2 • HS-USB WWAN Adapter 90B2
AT interface	AT commands handler applies the proper line termination sequence "\r\n" to all supported AT commands.	AT commands handler applies the uncorrected line termination sequence "\n\r" in the +CSGT URC and some AT commands in test mode like "AT+UPSV=?", "AT+UFOTA=?" plus some others related to the LWM2M functionality.	AT commands handler applies the uncorrected line termination sequence "\n\r" in the +CSGT URC and some AT commands in test mode like "AT+UPSV=?", "AT+UFOTA=?" plus some others related to the LWM2M functionality.	AT commands handler applies the uncorrected line termination sequence "\n\r" in the +CSGT URC and some AT commands in test mode like "AT+UPSV=?", "AT+UFOTA=?" plus some others related to the LWM2M functionality.
+USIO	Serial interfaces configuration options: • 0: AT="UART" • 1: AT="UART"; AT="AUX UART" • 4: AT="UART"; GNSS="AUX UART"[3]	n.a.	n.a.	n.a.
+UUARTCONF	Available for AUX UART configuration	n.a.	n.a.	n.a.
+CFUN (options)	0, 1, 4, 5, 15, 16, 19	0, 1, 4, 5, 15	0, 1, 4, 5, 15	0, 1, 4, 5, 15
+UMNOPROF	• Default MNO profile: 90 (global) • MNO profile 0 (undefined): n.a. • To restore the settings to the factory programmed values for the specific profile, the profile can be	• Default MNO profile: 0 (undefined) • To restore the settings to the factory programmed values for the specific profile, the profile shall be changed via +UMNOPROF set	• Default MNO profile: 28 (Softbank) on "63B", 39 (SKT) on "73B", 4 (Telstra) on "83B" • To restore the settings to the factory programmed values for the specific profile, the profile shall be	• Default MNO profile: 0 (undefined) • To restore the settings to the factory programmed values for the specific profile, the profile shall be changed via +UMNOPROF set

---

[3] Not supported by SARA-R422

Command or feature	SARA-R422 / SARA-R422S / SARA-R422M8S	SARA-R412M-02B-03	SARA-R410M-63B / SARA-R410M-73B / SARA-R410M-83B	SARA-R410M-02B-03
	reapplied with UMNOPROF set command.	command and set back to the current value.	changed via +UMNOPROF set command and set back to the current value.	command and set back to the current value.
+UBANDMASK (options)	(0-2),18446744073709551615, 18446744073709551615	(0-1),0xffffffffffffffff,0xffffffffffffffff	(0-1),0xffffffffffffffff,0xffffffffffffffff	(0-1),0xffffffffffffffff,0xffffffffffffffff
+URAT (options)	7, 8, 9	7, 8, 9	7, 8[4]	7, 8
<AcT> support in: +COPS +CREG +CGREG	0, 3, 7, 9	0, 3, 7, 9	7, 9	7, 9
+COPS	<mode>=0 (automatic) in set functionality does not reset the selected RATs configuration	<mode>=0 (automatic) in set functionality does reset the selected RATs configuration	<mode>=0 (automatic) in set functionality does reset the selected RATs configuration	<mode>=0 (automatic) in set functionality does reset the selected RATs configuration
+CGACT	Always issue the AT+CGACT=1,<cid> command on used context <cid> even if the +CGDCONT AT command returns that the context is still active with a valid IP address. This is highly recommended to activate the PS data connection avoiding possible conflicts between applications.	Optional	Optional	Optional
+UPSV (options)	0, 3, 4	0, 4	0, 4	0, 4
+UPSMVER (options)	4, 8	1, 2, 4, 8	1, 2, 4, 8	1, 2, 4, 8
+UCGED (options)	0, 2 The option 5 is considered as a redundant syntax: accordingly it has been dropped.	0, 2, 5	0, 2, 5	0, 2, 5
SMS URCs with MUX	Available	n.a.	n.a.	n.a.
ePCO disabling	+UCFGCIOT AT command	Suitable MNO profile 101	Suitable MNO profile 101 in SARA-R410M-83B only	Suitable MNO profile 101

[4] Not supported by SARA-R410M-63B and SARA-R410M-73B product versions

Command or feature	SARA-R422 / SARA-R422S / SARA-R422M8S	SARA-R412M-02B-03	SARA-R410M-63B / SARA-R410M-73B / SARA-R410M-83B	SARA-R410M-02B-03
+ULWM2MSTAT URC	Applied syntax (no spaces between the provided values) +ULWM2MSTAT: <event>,<param1>[,<param2>]	Applied syntax (spaces between the provided values) +ULWM2MSTAT: <event>, <param1>[, <param2>]	Applied syntax (spaces between the provided values) +ULWM2MSTAT: <event>, <param1>[, <param2>]	Applied syntax (spaces between the provided values) +ULWM2MSTAT: <event>, <param1>[, <param2>]
+UFOTASTAT URC	Applied syntax (no spaces between the provided values) +UFOTASTAT: <event>,<param1>[,<param2>]	Applied syntax (spaces between the provided values) +UFOTASTAT: <event>, <param1>[, <param2>]	Applied syntax (spaces between the provided values) +FOTASTAT: <event>, <param1>[, <param2>]	Applied syntax (spaces between the provided values) +UFOTASTAT: <event>, <param1>[, <param2>]
+UPSMR URC	Applied syntax (no spaces between the provided values) +UPSMR: <state>[,<param1>]	Applied syntax (spaces between the provided values) +UPSMR: <state>[,<param1>]	Applied syntax (spaces between the provided values) +UPSMR: <state>[,<param1>]	Applied syntax (spaces between the provided values) +UPSMR: <state>[,<param1>]
+UBKUPDATA	• restore of module unique data • not restored user files, parameters and profiles (customer settings)	• restore of module unique data • restore of the whole file system (customer settings too)	n.a.	• restore of module unique data • restore of the whole file system (customer settings too)
+UFACTORY	available	n.a.	n.a.	n.a.
Security	available[5]	n.a.	available	n.a.
Internal GNSS	available[6]	n.a.	n.a.	n.a.
CellLocate®	available[5]	available	available	available

Table 17: Software migration guide from SARA-R412M and SARA-R410M

---

[5] Not supported by SARA-R422
[6] Not supported by SARA-R422 and SARA-R422S

Appendix

A Glossary

Abbreviation	Definition
CHAP	Challenge handshake authentication protocol
DCE	Data Circuit-terminating Equipment* / Data Communication Equipment*
DL	Down Link (Reception)
DRX	Discontinuous Reception
DTE	Data Terminal Equipment
eDRX	Extended DRX
FW	Firmware
HW	Hardware
LPWAN	Low Power Wide Area Network
LwM2M	Lightweight M2M
MNO	Mobile Network Operator
MO	Mobile Originated
MT	Mobile Terminated
NVM	Non-Volatile Memory
NW	Network
OPLMN	Operator Public Land Mobile Network
PAP	Password authentication protocol
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PSM	Power Saving Mode
RAT	Radio access technology
RPLMN	Registered Public Land Mobile Network
SW	Software
TAU	Tracking Area Update
UE	User Equipment
URC	Unsolicited Result Code

Table 18: Explanation of the abbreviations and terms used

Related documentation

[1]   u-blox SARA-R4 series data sheet, UBX-16024152
[2]   u-blox SARA-R4 series AT commands manual, UBX-17003787
[3]   u-blox SARA-R4 series system integration manual, UBX-16029218
[4]   u-blox SARA-R4 FW update application note, UBX-17049154
[5]   u-blox Internet applications development guide application note, UBX-20032566
[6]   u-blox IoT Security-as-a-Service application note, UBX-20013561
[7]   u-blox SARA-R4 / SARA-R5 GNSS implementation application note, UBX-20012413
[8]   u-blox Mux implementation in cellular modules application note, UBX-13001887
[9]   u-blox LwM2M objects and commands application note, UBX-18068860
[10]   u-blox SARA-R5 SARA-R422 AWS IoT Core_ application note, UBX-20044809
[11]   u-blox EVK-R4 user guide, UBX-16029216
[12]   3GPP TS 24.008 - Mobile radio interface layer 3 specification
[13]   3GPP TS 27.010 V3.4.0 - Terminal Equipment to User Equipment (TE-UE) multiplexer protocol (Release 1999)
[14]   GSMA TS.34 IoT Device Connection Efficiency Guidelines

☞ For regular updates to u-blox documentation and to receive product change notifications, register on our homepage (www.u-blox.com).

Revision history

Revision	Date	Name	Comments
R01	27-Apr-2021	fdil	Initial release
R02	09-Jul-2021	fdil	IP release

Contact

For complete contact information, visit us at www.u-blox.com.

u-blox Offices

North, Central and South America

u-blox America, Inc.

Phone: +1 703 483 3180
Email: info_us@u-blox.com

Regional Office West Coast:

Phone: +1 408 573 3640
Email: info_us@u-blox.com

Technical Support:

Phone: +1 703 483 3185
Email: support@u-blox.com

**Headquarters
Europe, Middle East, Africa**

u-blox AG

Phone: +41 44 722 74 44
Email: info@u-blox.com
Support: support@u-blox.com

Asia, Australia, Pacific

u-blox Singapore Pte. Ltd.

Phone: +65 6734 3811
Email: info_ap@u-blox.com
Support: support_ap@u-blox.com

Regional Office Australia:

Phone: + 61 3 9566 7255
Email: info_anz@u-blox.com
Support: support_ap@u-blox.com

Regional Office China (Beijing):

Phone: +86 10 68 133 545
Email: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Chongqing):

Phone: +86 23 6815 1588
Email: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shanghai):

Phone: +86 21 6090 4832
Email: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shenzhen):

Phone: +86 755 8627 1083
Email: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office India:

Phone: +91 80 405 092 00
Email: info_in@u-blox.com
Support: support_in@u-blox.com

Regional Office Japan (Osaka):

Phone: +81 6 6941 3660
Email: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Japan (Tokyo):

Phone: +81 3 5775 3850
Email: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Korea:

Phone: +82 2 542 0861
Email: info_kr@u-blox.com
Support: support_kr@u-blox.com

Regional Office Taiwan:

Phone: +886 2 2657 1090
Email: info_tw@u-blox.com
Support: support_tw@u-blox.com