AN13512

Kinetis Wireless Family Products Bluetooth Low Energy Coexistence with Wi-Fi Application

Rev. 0 — 10 March 2022 Application note

Document information

Information	Content
Keywords	Kinetis, Wireless, Bluetooth, BLE, Wi-Fi
Abstract	This application note provides the KW3x/4x Bluetooth Low Energy family productsimmunity on Wi-Fi signals and methods to improve coexistence with Wi-Fi.

1 Introduction

This application note provides the KW3x/4x Bluetooth Low Energy family products immunity on Wi-Fi signals and methods to improve coexistence with Wi-Fi.

Section 2 gives an overview of Wi-Fi immunity without any specific suppression techniques. For details, see *EVK-KW45 Co-existence with RF System Evaluation Report for the Bluetooth LE applications* (document AN13229).

Section 3 refers to the objective of the coexistence strategy to prevent Wi-Fi and Radio from transmitting simultaneously. To prevent the Radio from receiving when the Wi-Fi transceiver owns the RF channel, a configuration option exists. NXP 2.4 GHz Radio IC supports the coexistence interface signals.

For more information, see *KW45B41Z reference manual* (document KW45B41ZRM).

2 Bluetooth LE immunity on Wi-Fi signal

This chapter provides an overview about Bluetooth LE performances against Wi-Fi signal. Those results are part of *AN13229 EVK-KW45 Co-existence with RF System Evaluation Report for the Bluetooth LE applications* (document AN13229). This document provides the RF evaluation test results of the KW45B41Z EVK for Bluetooth LE applications (2FSK modulation). It includes the test setup description and the tools used to perform the tests on your own. To get the KW45 radio parameters, see *KW45B41Z data sheet* (document KW45B41Z).

This section describes the test method overviews and results to Packet Error Rate (PER) depending on the Wi-Fi interferer (Adjacent Carrier Interferers and Co-channel).

2.1 Test bench

This bench setup is performed with the KW45B41Z-EVK for example. It also works for other FRDM-KW3x/4x boards.

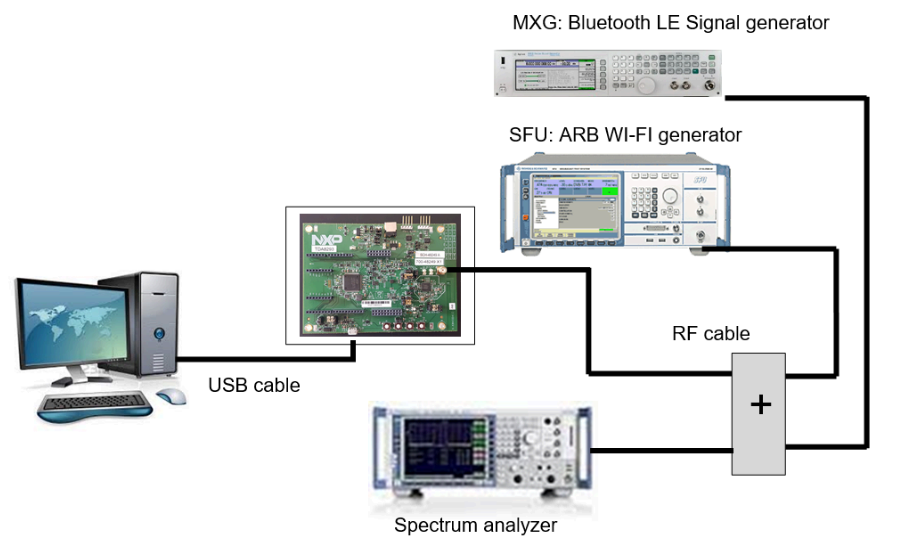

Figure 1. Test bench setup

2.2 Software

Before measuring, load a binary code (connectivity software) into the flash memory of the board.

To load the code with KW45B41Z EVK, see NXP® Evaluation Kit for Kinetis® KW45B41Z MCUs. The binary code used for the following tests is the Connectivity Software package GenFSK protocol (2FSK modulation). The TERATERM terminal emulator is used to communicate with the KW45 MCU.

2.3 Wi-Fi interferences - ACIs

This section describes the test methods and results to Packet Error Rate (PER) using the Wi-Fi interferer, Adjacent Carrier Interferers (ACI).

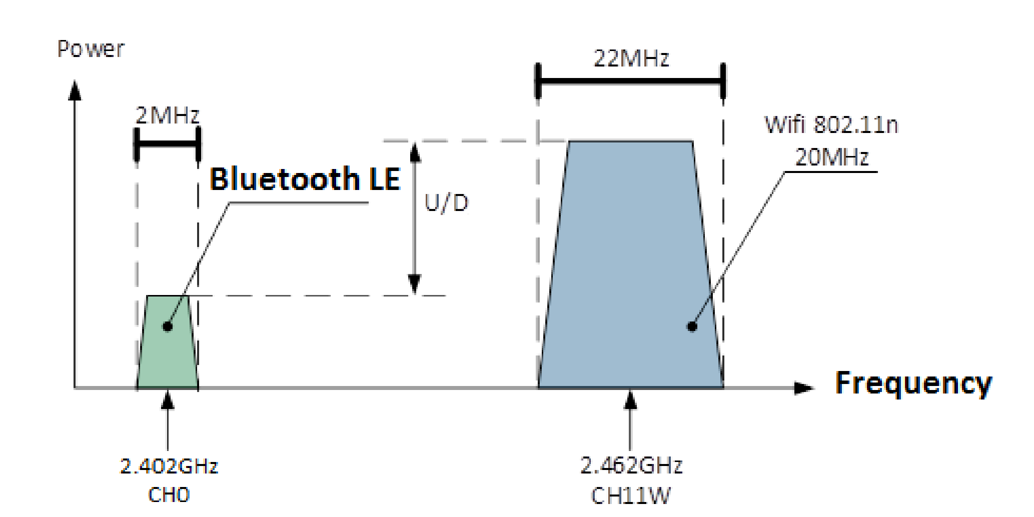

Figure 2. Wi-Fi interferer – ACIs

2.3.1 ACIs test method

- Set the KW45 radio to:
  - RX mode (Bluetooth LE 1 Msps, 2 Msps, 500 Ksps, or 125 Ksps),
  - Modulated
  - Continuous mode
  - Frequency: channel 0 (2.402 MHz)
- Set the generator to:
  - Bluetooth LE modulated signal (typical 1500 packets of 37 bytes payload)
  - Continuous mode
  - Frequency: channel 0 (2.402 MHz).
- Set the analyzer for power calibration on Bluetooth LE signal and Wi-Fi signal.
- Wi-Fi signal (BW = 22 MHz) is set from a level of -40 dBm to 0 dBm, channel 11 (2.462 GHz), and channel 6 (2.437 GHz).
- Bluetooth LE power is decreased until PER criteria (< 30.8 %) is reached.

2.3.2 ACIs result

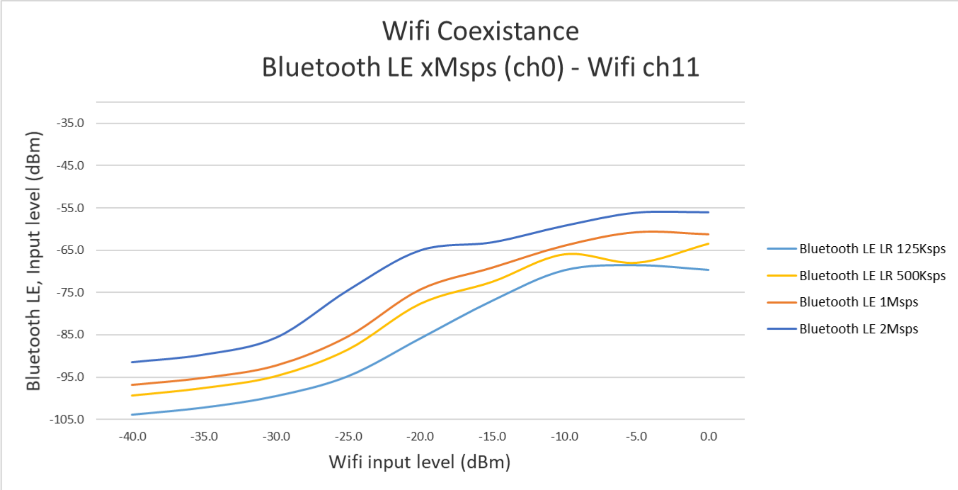

Figure 3. Bluetooth LE and Wi-Fi coexistence (ACIs)

2.4 Wi-Fi interferences – Co-channel

This section describes the test methods and results to Packet Error Rate (PER) using the Wi-Fi interferer co-channel.

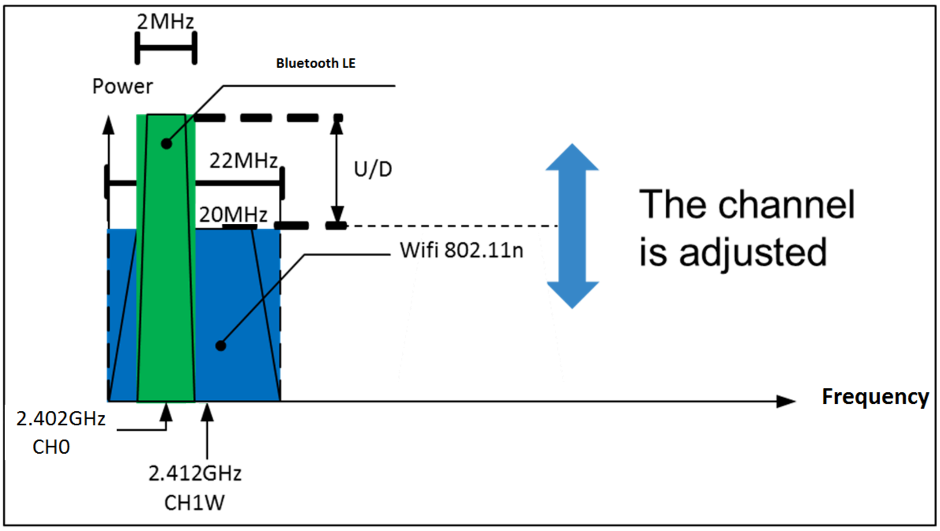

Figure 4. Wi-Fi interferer – Co-channel

2.4.1 Co-channel test method

- Set the KW45 radio to:
  - RX mode (Bluetooth LE 1 Msps, 2 Msps, 500 Ksps, or 125 Ksps)
  - Modulated
  - Continuous mode
  - Frequency: Channel 0 (2.402 MHz)
- Set the generator to:
  - Bluetooth LE modulated signal (typical 1500 packets of 37 bytes payload)

- Continuous mode
- Frequency: channel 0 (2.402 MHz)

- Set the analyzer for power calibration on Bluetooth LE signal and Wi-Fi signal.
- Wi-Fi signal (BW = 22 MHz) is set from a level of -40 dBm to 0 dBm, channel 1 (2.412 GHz).
- Bluetooth LE power is decreased until PER criteria (< 30.8 %) is reached.

2.4.2 Co-channel results

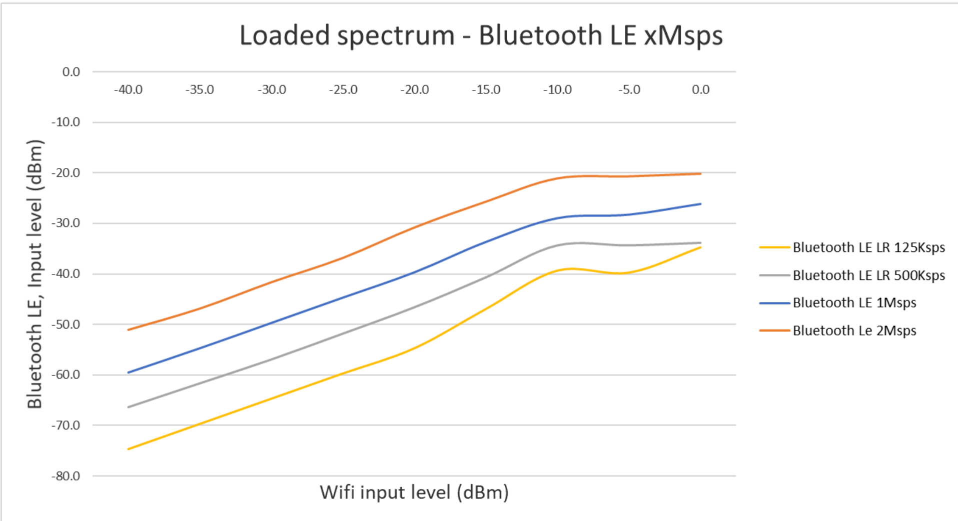

Figure 5. Bluetooth LE and Wi-Fi co-channel

3 Co-existence strategy

This chapter covers the coexistence strategy to prevent Wi-Fi and Radio from transmitting simultaneously. To prevent the Radio from receiving when the Wi-Fi transceiver owns the RF channel, a configuration option exists. The 2.4 GHz Radio IC of NXP supports the coexistence interface signals.

For more details, see *KW45B41Z reference manual* (document KW45B41ZRM).

3.1 Wi-Fi coexistence interface

Hardware and software methods allow the radio to coexist in the same space as a Wi-Fi transceiver IC. They share 2.4 GHz frequency band. The coexistence scheme designates the Wi-Fi transceiver as the master and Radio as the slave. The coexistence strategy prevents Wi-Fi and Radio from transmitting simultaneously. To prevent the Radio from receiving when the Wi-Fi transceiver owns the RF channel, a configuration option exists.

The 2.4 GHz radio IC supports the coexistence interface signals, as shown in Figure 6. In a typical application, only a subset is used.

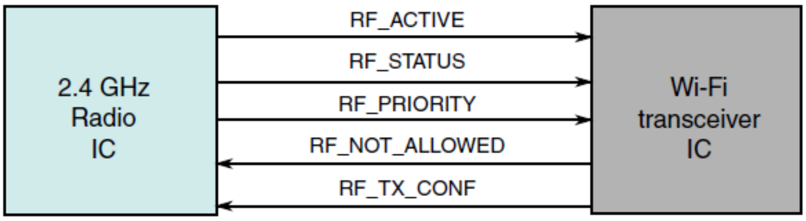

Figure 6. Wi-Fi coexistence interface

The 2.4 GHz radio architecture supports a flexible coexistence interface. The interface enables the Narrow Band (NB) radio (for example, Bluetooth and proprietary protocols) to coexist in the same space as a Wi-Fi radio, which shares frequency band, or a different IC, with which active synchronization may be required to reduce either power consumption from battery or reduce Electronic Magnetic Interference (EMI). As a simplification, this section primarily showcases the coexistence capabilities of the NB 2.4 GHz radio in the context of Wi-Fi radio coexistence.

Note: *An Inter-Processor Communication (IPC) channel using a serial bus may also be used to augment the capabilities of the HW coexistence interface.*

Typical coexistence schemes between a Bluetooth and Wi-Fi designate the Wi-Fi transceiver as the master and the 2.4 GHz transceiver as the slave. However in some cases, an application profile may dictate the opposite. The coexistence strategy is to prevent both the NB 2.4 GHz radio and the Wi-Fi radio from transmitting simultaneously. To prevent the NB 2.4 GHz radio from reception when the Wi-Fi radio owns the RF channel, a configuration option exists. Yet another implementation choice is for the two radios to indicate the nature of their RF activity. It allows the coexistence scheme for simultaneous reception on both radios as well as other options when NB and Wi-Fi channels have adequate separation.

For more details, see **Chapter 46.2.5 Wi-Fi Coexistence Interface** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.2 Coexistence pin definition

Table 1 describes the Wi-Fi coexistence pins.

Table 1. Coexistence pin definition

Wi-Fi coexistence function	Pin direction	Pin description
`RF_ACTIVE` (REQUEST)	O	An output is asserted prior to any Radio event and remains asserted during the event.
`RF_STATUS` (DIRECTION)	O	An output indicates when the Radio is in an RX or TX even, software can directly control this signal.
`RF_PRIORITY`	O	An output indicates to the external Wi-Fi device that the radio event is a high priority and it needs access to the 2.4 GHz antenna.
`RF_NOT_ALLOWED` (!GRANT)	I	External signal causes the internal Radio to crease radio activity.

Table 1. Coexistence pin definition*...continued*

Wi-Fi coexistence function	Pin direction	Pin description
RF_TX_CONF	I	Signal from an external Radio which indicates the availability of the 2.4 GHz antenna to the internal Radio. ***Note:*** *This signal is not connected to the radio hardware. Radio software can use any interrupt-capable GPIO which the application assigns for this function.*

Register: `RF2p4GHz_COEXT`, Offset: 20 h

Selects the source for `RF_GPO[7:0]`.

In description below,

```
coext[3:0] = {rf_priority[1:0], rf_status,rf_active}
000b - RF_GPO[7:0] = {coext[3:0], fem_ctrl[3:0]}
001b - RF_GPO[7:0] = {fem_ctrl[3:0], coext[3:0]}
010b - RF_GPO[7:0] = {lant_lut_gpio[3:0], fem_ctrl[3:0]}
011b - RF_GPO[7:0] = {fem_ctrl[3:0], lant_lut_gpio[3:0]}
100b - RF_GPO[7:0] = {lant_lut_gpio[3:0], coext[3:0]}
101b - RF_GPO[7:0] = {coext[3:0], lant_lut_gpio[3:0]}
```

Table 2. RF_GPO muxing

RF GPO muxing:
RF_GPO_0 /1/ 2/ 3: Select FEM/Coexistence (w/o RF_NOT_ALLOWED)/External antenna switching
RF_GPO_4 /5 / 6 / 7: Select FEM/Coexistence (w/o RF_NOT_ALLOWED)/External antenna switching
RF_GPO_8/9/10/11: Select FEM/External antenna switching

Table 3. RF_GPO bit register

40 QFN	48 QFN	Pin name	ALT3	ALT4	ALT6	ALT7	ALT8	ALT9	Wake-up
7	8	PTA2		RF_GPO_11					
8	9	PTA3		RF_GPO_10					
9	10	PTA4	RF_GPO_9						
		PTA5							
	11	PTA16				RF_GPO_8			**RF_NOT_ALLOWED**
10	12	PTA17				RF_GPO_7	RF_GPO_8		WUU)_P3/**RF_NOT_ALLOWED**

Table 3. RF_GPO bit register*...continued*

40 QFN	48 QFN	Pin name	ALT3	ALT4	ALT6	ALT7	ALT8	ALT9	Wake-up
11	13	PTA18			RF_GPO_0				
12	14	PTA19			RF_GPO_1				
15	17	PTA20			RF_GPO_2				
16	18	PTA21			RF_GPO_3	RF_GPO_7		RF_GPO_10	
	24	PTD1		RF_GPO_4					
	25	PTD2		RF_GPO_5					
	26	PTD3		RF_GPO_6					
36	45	PTC7							WUUO_P12/NMI_b/**RF_NOT_ALLOWED**

Behavioral control information for the radio pins is provided below. See **Radio Coexistence/FEM/LANT Connections** which illustrates how the signals are connected and muxed in the radio in *KW45B41Z reference manual* (document KW45B41ZRM).

For more details, see **Chapter 56.3.4.6.1 Coexistence Pin Definition** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.3 Coexistence signaling options

Figure 7 illustrates Bluetooth and Wi-Fi coexistence signaling (adapted from Wi-Fi alliance documentation). The interface definition between the two radios has evolved over time targeting improved spectral and antenna control efficiency. Most modern BT and Wi-Fi interfaces utilize three or more signals.

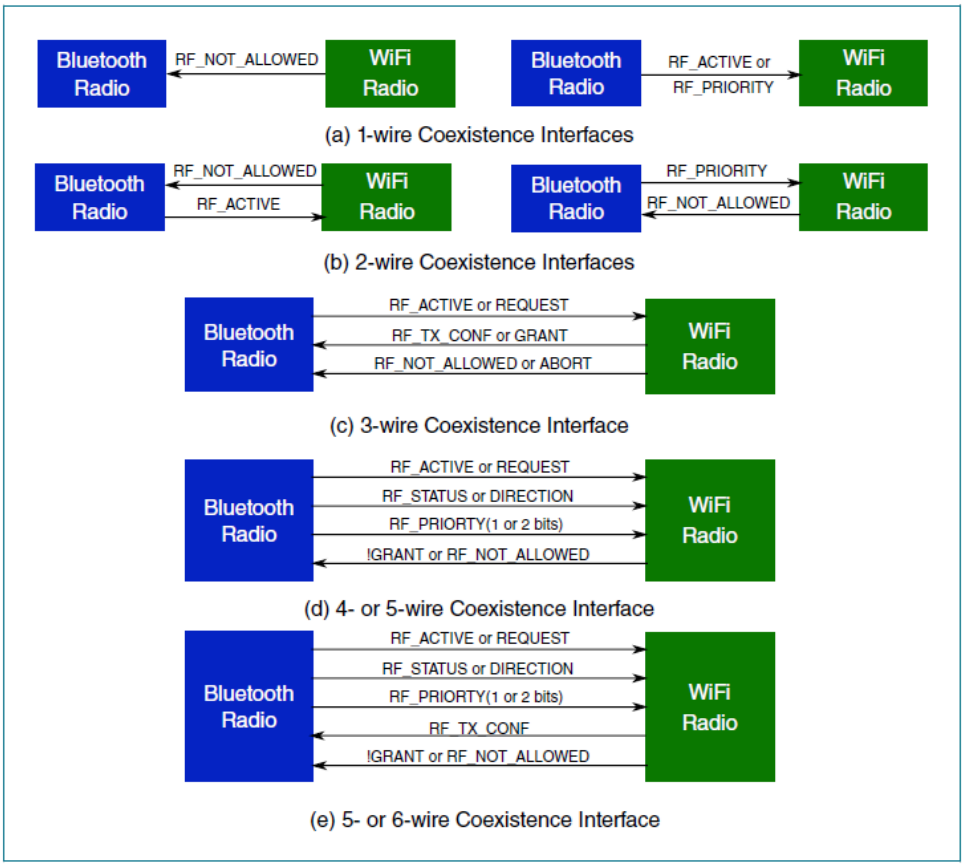

Figure 7. Coexistence signaling options between Bluetooth LE and Wi-Fi radios

For more details, see **Chapter 56.3.4.6.2 Coexistence Signaling Options** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.4 Example coexistence pin mapping

Table 4 lists example mapping of legacy coexistence signals supported by the NB 2.4 GHz radio for a few Wi-Fi radios available in the market.

Table 4. Example coexistence pin mapping

Wi-Fi co-existence use case	RF_ACTIVE	RF_STATUS	RF priority	RF_NOT_ALLOWED	RF_TX_CONF	Wi-Fi SoC
Direction	Output	Output	Output	Input	Input	

Table 4. Example coexistence pin mapping...*continued*

Wi-Fi co-existence use case	RF_ACTIVE	RF_STATUS	RF priority	RF_NOT_ALLOWED	RF_TX_CONF	Wi-Fi SoC
Functionality	• Indicates a radio event; • Must stay asserted during a radio event; • De-asserted if `RF_NOT_ALLOWED` = 1.	• Indicates RX/TX event; • Optionally `RF_Priority` signal can be mixed on it.	• Specifies `RF_ACTIVE`; prior to an external traffic arbiter.	• Indicates an external command for the NB radio to cease radio activity.	• Indicates grant of antenna to TX; • Must sample if `RF_Priority` requested. • Can be any GPIO.	
1-wire interface, WLAN is Master				×		
1-wire interface, BT is Master	×					
2-wire interface, Cross signaling between BT and WLAN	×			×		
2-wire interface, BT priority and WLAN TX signaling			×		×	
3-wire: Third-party interface	×			×	×	Broadcom, CSR
3-wire: Request, Grant, and Status	×	×			×	BRCM43XX; Nokia 3-wire option
3-wire: Qualcomm	×		×	O	×	QCOM Dakota chipset

Table 4. Example coexistence pin mapping*...continued*

Wi-Fi co-existence use case	RF_ACTIVE	RF_STATUS	RF priority	RF_NOT_ALLOWED	RF_TX_CONF	Wi-Fi SoC
4-wire: Request, Grant, Status, and Freq (Nokia 4-wire option)	×	×	×		×	BCM89xx; Nokia 4-wire option
4-wire: CSR interface	×	×	×	O	×	CSR-BC41BXX
4-wire: Phillips interface	×	×		×	×	

For more details, see **Chapter 56.3.4.6.3 Example Coexistence Pin Mapping** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.5 Wi-Fi coexistence

Provisions allow the 2.4 GHz transceiver to coexist in the same space as a Wi-Fi transceiver IC, which shares the frequency band. The coexistence scheme designates the Wi-Fi transceiver as the master and the 2.4 GHz transceiver as the slave. The objective of the coexistence strategy is to prevent both the Wi-Fi and 2.4 GHz transceivers transmitting simultaneously. To prevent the 2.4 GHz transceiver from receiving when the Wi-Fi transceiver owns the RF channel, a configuration option exists.

The 2.4 GHz Radio IC supports the coexistence interface signals, as shown in Figure 9. A typical application only uses a subset.

The Wi-Fi IC generates a signal, `RF_NOT_ALLOWED`. If this signal is asserted, then 2.4 GHz radio does not perform any communication. When this signal is de-asserted, 2.4 GHz radio is free to perform communications.

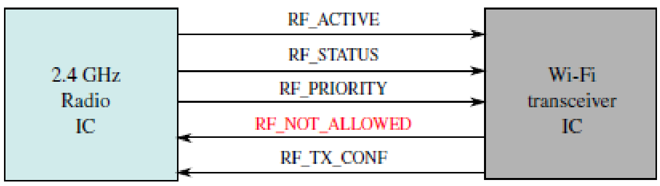

Figure 8. Wi-Fi coexistence pins definition

When `RF_NOT_ALLOWED` aborting is enabled, the GENERIC_FSK Link Layer hardware must respond to `RF_NOT_ALLOWED` assertions:

- Abort any TX or RX sequence which is underway.
- Link Layer software must not initiate any new sequences until `RF_NOT_ALLOWED` is de-asserted.

Link Layer handles the hardware response autonomously, with no MCU intervention required.

In the multiprotocol 2.4 GHz radio, RF_NOT_ALLOWED aborting can be individually enabled/disabled for each protocol engine. For GENERIC_FSK, RF_NOT_ALLOWED_EN[3] is the associated enable control bit. This bit resides in the COEX_CTRL register in XCVR address space.

- When this bit is **0**, transitions on RF_NOT_ALLOWED are ignored by the GENERIC_FSK Link Layer hardware.
- When this bit is **1**, the GENERIC_FSK Link Layer hardware monitors RF_NOT_ALLOWED and aborts any active sequence which is underway when an assertion on the pin occurs.

The complete hardware response to RF_NOT_ALLOWED assertions is described below.

- RF_NOT_ALLOWED_NO_TX and RF_NOT_ALLOWED_NO_RX control bits provide additional control over RF_NOT_ALLOWED aborting.
  - If RF_NOT_ALLOWED_NO_TX = 1, an RF_NOT_ALLOWED abort occurs only if a GENERIC_FSK TX sequence is underway (generic_fsk_tx_en=1). GENERIC_FSK TX sequence is not aborted if RF_NOT_ALLOWED_NO_TX = 0.
  - If RF_NOT_ALLOWED_NO_RX = 1, an RF_NOT_ALLOWED abort occurs only if GENERIC_FSK RX sequence is underway (generic_fsk_rx_en = 1). GENERIC_FSK RX sequence is not aborted if RF_NOT_ALLOWED_NO_RX = 0.
- RF_NOT_ALLOWED_NO_TX and RF_NOT_ALLOWED_NO_RX control bits reside in the COEX_CTRL register.

To trigger a hardware abort, use the pll_abort input to the GENERIC_FSK Link Layer hardware. The reason is that the hardware response to the RF_NOT_ALLOWED assertion is identical to that of a PLL unlock event. It also means when RF_NOT_ALLOWED aborting is enabled for GENERIC_FSK, the PLL_UNLOCK_IRQ interrupt status bit indicates a PLL unlock condition and a RF_NOT_ALLOWED abort. PLL aborting and RF_NOT_ALLOWED aborting are enabled separately, with the COEX_CTRL register maintaining the control bits required for the latter. The status bits for RF_NOT_ALLOWED aborting are available in COEX_CTRL. Therefore, if both PLL and RF_NOT_ALLOWED aborting are enabled, software can distinguish the source of the PLL_UNLOCK_IRQ.

The sequence of events results in a hardware abort of an GENERIC_FSK TX operation triggered by an assertion on RF_NOT_ALLOWED. It is a collaboration between the Transceiver Sequence Manager (TSM) and the GENERIC_FSK Link Layer hardware, as shown in Figure 9.

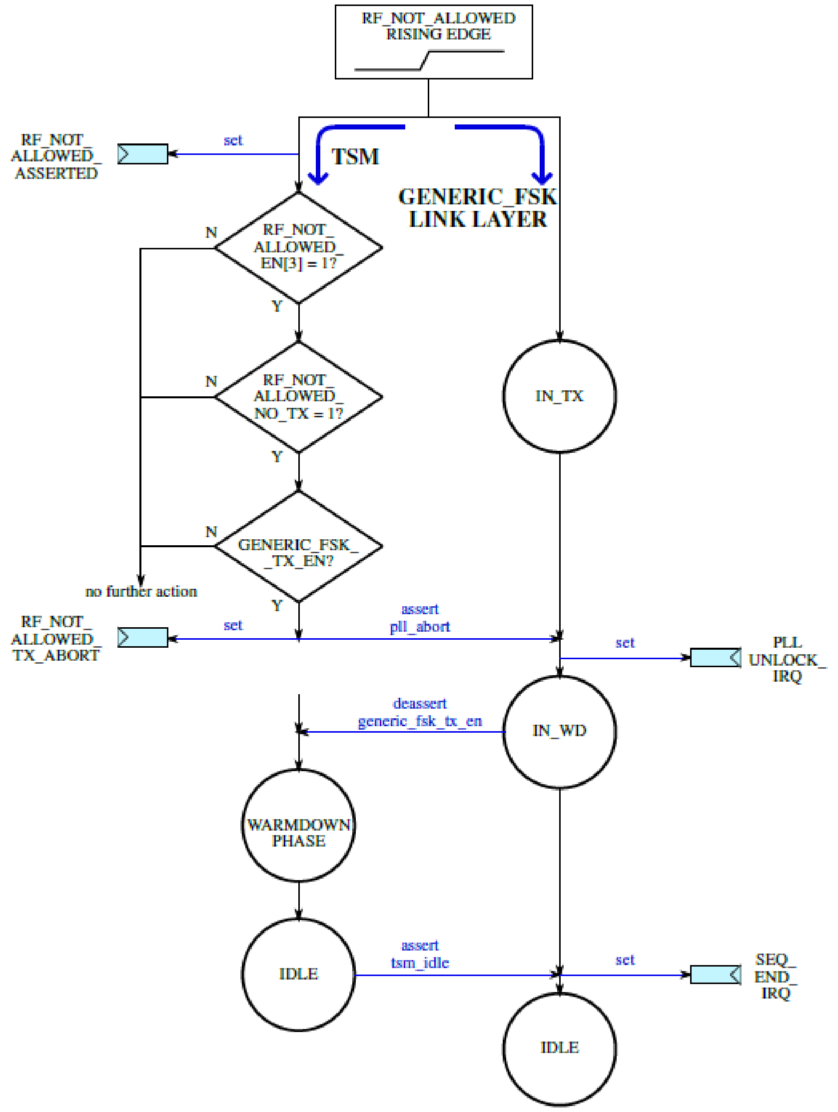

Figure 9. Sequence of events - GENERIC_FSK TX operation triggered

Upon assertion on `RF_NOT_ALLOWED`, the TSM sets the `RF_NOT_ALLOWED_ASSERTED` status bit in `COEX_CTRL` and checks whether the conditions for a hardware abort are all met:

- `RF_NOT_ALLOWED_EN[3]` = 1, which enables `GENERIC_FSK` to respond to `RF_NOT_ALLOWED` events.
- `RF_NOT_ALLOWED_NO_TX` = 1, which enables TX operations to be aborted.
- `generic_fsk_tx_en` = 1, TX request to TSM from `GENERIC_FSK`, indicating that TX operation is in progress.

If all conditions are not met, no further action is taken. Otherwise, the TSM sets `COEX_CTRL[RF_NOT_ALLOWED_TX_ABORT]` and asserts `pll_unlock` to the `GENERIC_FSK` Link Layer hardware. `GENERIC_FSK` responds by asserting `IRQ_CTRL[PLL_UNLOCK_IRQ]` in GENERIC_FSK address space. `GENERIC_FSK` enters `IN_WD` state, which de-asserts `generic_fsk_tx_en` to the TSM. It initiates the TSM TX warm-down. `GENERIC_FSK` holds in `IN_WD` to wait for TSM to return to idle.

Once this case occurs, `GENERIC_FSK` asserts `IRQ_CTRL[SEQ_END_IRQ]` and returns to its IDLE state. Three status bits are now set to indicate to software that the source of the abort is an `RF_NOT_ALLOWED` assertion:

- IRQ_CTRL[PLL_UNLOCK_IRQ]
- COEX_CTRL[RF_NOT_ALLOWED_ASSERTED]
- COEX_CTRL[RF_NOT_ALLOWED_TX_ABORT]

The sequence of events results in a hardware abort of an GENERIC_FSK RX sequence triggered by an assertion on RF_NOT_ALLOWED, as shown in Figure 10.

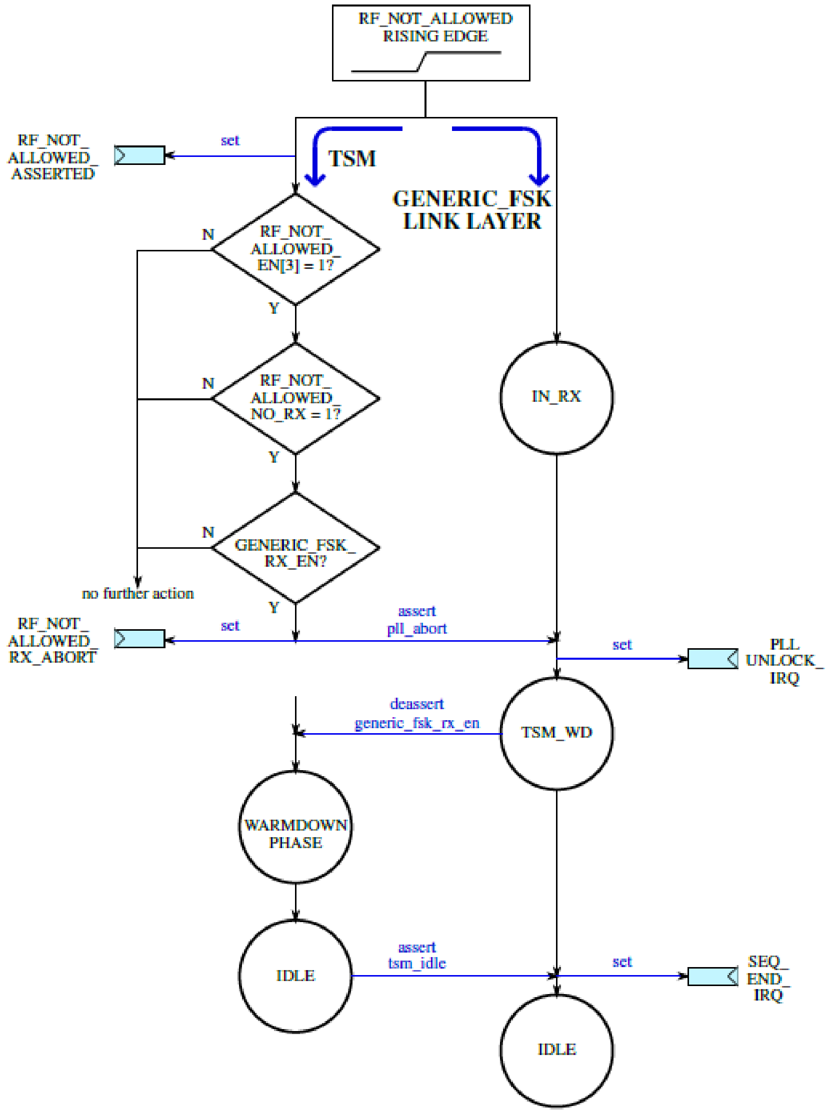

Figure 10. Sequence of events - GENERIC_FSK RX operation triggered

Upon assertion on `RF_NOT_ALLOWED`, the TSM sets the `RF_NOT_ALLOWED_ASSERTED` status bit in `COEX_CTRL` and checks that the conditions for a hardware abort are all met:

- `RF_NOT_ALLOWED_EN[3]` = 1, which enables `GENERIC_FSK` to respond to `RF_NOT_ALLOWED` events.
- `RF_NOT_ALLOWED_NO_RX` = 1, which enables RX operations to be aborted.

- generic_fsk_rx_en = 1, RX request to TSM from GENERIC_FSK, indicating that RX operation is in progress.

If all conditions are not met, no further action is taken. Otherwise, the TSM sets COEX_CTRL[RF_NOT_ALLOWED_RX_ABORT] and asserts pll_unlock to the GENERIC_FSK Link Layer hardware. GENERIC_FSK responds by asserting IRQ_CTRL[PLL_UNLOCK_IRQ] in GENERIC_FSK address space. GENERIC_FSK enters IN_WD state, which de-asserts generic_fsk_rx_en to the TSM. It initiates the TSM TX warm-down. GENERIC_FSK holds in IN_WD to wait for TSM to return to idle.

Once this case occurs, GENERIC_FSK asserts IRQ_CTRL[SEQ_END_IRQ] and returns to its IDLE state. Three status bits are now set to indicate to software that the source of the abort was an RF_NOT_ALLOWED assertion:

- IRQSTS1[PLL_UNLOCK_IRQ]
- COEX_CTRL[RF_NOT_ALLOWED_ASSERTED]
- COEX_CTRL[RF_NOT_ALLOWED_RX_ABORT]

For more details, see **Chapter 56.3.7.1.4.14 Wi-Fi Coexistence** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.5.1 RF_NOT_ALLOWED behavioral control

The Wi-Fi IC generates a signal, RF_NOT_ALLOWED. If this signal is asserted, the 2.4 GHz radio does not perform any communication. When this signal is de-asserted, the 2.4 GHz radio is free to perform communications. When the RF_NOT_ALLOWED signal is asserted and 2.4 GHz radio has already initiated the transmission/reception of a packet, the 2.4 GHz radio must stop its activity immediately.

Note: *Radio supports a software override of the RF_NOT_ALLOWED signal. Radio can be used for debug. It can also enable the capability to abort radio activity under software control (based on application layer arbitration between a multi-radio system).*

As of the Gen 4.5 radio, the RF_NOT_ALLOWED is not qualified by the TSM. The link layer(s) directly use the RF_NOT_ALLOWED signal. Appropriate action is taken to de-assert their tx_en or rx_en signal as needed.

Table 5 describes register bits in the RFMC and RADIO_MISC to enable, control, and provide status for RF_NOT_ALLOWED.

Table 5. RF_NOT_ALLOWED behavioral control

Field	Type	Description
RFNA_IBE[2:0]	RW	RFMC bit field to select which (among several) SOC pin to use for RF_NOT_ALLOWED function
RF_NOT_ALLOWED_EN[3:0]	RW	RADIO_MISC (COEX_CTRL register) bit field to choose which link layers receive RF_NOT_ALLOWED signal
RF_NOT_ALLOWED_ASSERTED	W1C	RADIO_MISC (COEX_CTRL register) bit field sets on assertion of RF_NOT_ALLOWED, cleared only by software
RF_NOT_ALLOWED	R	RADIO_MISC (COEX_CTRL register) bit field reflects the raw state of the selected RF_NOT_ALLOWED SOC pin
RF_NOT_ALLOWED_OVRD_EN	RW	RADIO_MISC (COEX_CTRL register) bit field. If set, allows software to control the RF_NOT_ALLOWED_OVRD bit field
RF_NOT_ALLOWED_OVRD	RW	RADIO_MISC (COEX_CTRL register) bit field. If RF_NOT_ALLOWED_OVRD_EN is set, the RF_NOT_ALLOWED signal to the link layers is driven with the value of the RF_NOT_ALLOWED_OVRD bit field.

Table 5. RF_NOT_ALLOWED behavioral control*...continued*

Field	Type	Description
RF_NOT_ALLOWED_INV	RW	RADIO_MISC (COEX_CTRL register) bit field. If set, the selected RF_NOT_ALLOWED pin is inverted before being used as the RF_NOT_ALLOWED signal to the link layers.

3.5.1.1 RF_ACTIVE behavioral control

The NB radio provides the RF_ACTIVE (REQUEST) output to request coexistence access. TSM, one of the link layers, or RFMC can generate this signal.

Table 6 describes register bits in the TSM, RFMC, and RADIO_MISC to enable, control, and provide status for RF_ACTIVE. For information on their **REQUEST** output, see the link layer chapters.

Table 6. RF_ACTIVE behavioral control

Field	Type	Description
RF_ACTIVE_RX_HI[7:0]	RW	TSM bit field to control when TSM RF_ACTIVE asserts in the RX sequence
RF_ACTIVE_RX_LO[7:0]	RW	TSM bit field to control when TSM RF_ACTIVE de-asserts in the RX sequence
RF_ACTIVE_TX_HI[7:0]	RW	TSM bit field to control when TSM RF_ACTIVE asserts in the TX sequence
RF_ACTIVE_TX_LO[7:0]	RW	TSM bit field to control when TSM RF_ACTIVE de-asserts in the TX sequence
TSM_RF_ACTIVE_OVRD_EN	RW	TSM bit field to provide override enable for TSM RF_ACTIVE output
TSM_RF_ACTIVE_OVRD	RW	TSM bit field to provide override value for TSM RF_ACTIVE output
TSM_SPARE1_EXTEND[7:0]	RW	TSM bit field to control how long TSM RF_ACTIVE remains asserted after the end of RX or TX sequence. This bit field is intended to close any gap which may occur between consecutive RX/TX operations.
COEX_SEL	RW	RADIO_MISC (COEX_CTRL register) bit field to select whether the TSM outputs (RF_ACTIVE, RF_STATUS, RF_PRIORITY) or the outputs of active link layer are input to the RFMC.
RFACT_SRC[1:0]	RW	RFMC bit field to select whether RF_ACTIVE radio output is driven by RFMC (2'b00). TSM/LL output from the COEX_SEL mux (2'b01), or Bluetooth LE bt_clk_req signal (2'b10)
RFACT_WKUP_DLY[5:0]	RW	RFMC bit field. If RFACT_SRC = 2'b00, this bit field configures number of 32 kHz reference clocks following enable of the XO to assert the RF_ACTIVE pin for a MAN/WOR/Bluetooth LE wake-up event.
RFACT_IDIS	RW	RFMC bit field. If RFACT_SRC = 2'b00, this bit field selects whether the RF_ACTIVE radio output de-asserts when TSM becomes idle.
RFACT_EN	RW	RFMC bit field. If RFACT_SRC = 2'b00, the RF_ACTIVE radio output is asserted while this bit is set.
RFACT_FLAG	W1C	RFMC bit field. Sets when the RF_ACTIVE radio output asserts.
RFACT_IE	RW	RFMC bit field. If set, the RFMC generates an interrupt to CM33 when the RF_ACTIVE radio output asserts.

3.5.1.2 RF_STATUS behavioral control

The NB radio provides the `RF_STATUS` (DIRECTION) output to indicate when the radio is in an RX or TX event. TSM or the active link layers can generate this signal.

Table 7 describes register bits in the TSM and `RADIO_MISC` to enable and control `RF_STATUS`. Refer to the link layer chapters for information on their **DIRECTION** output.

Table 7. RF_STATUS behavioral control

Field	Type	Description
`RF_STATUS_RX_HI[7:0]`	RW	TSM bit field to control when TSM `RF_STATUS` asserts in the RX sequence
`RF_STATUS_RX_LO[7:0]`	RW	TSM bit field to control when TSM `RF_STATUS` de-asserts in the RX sequence
`RF_STATUS_TX_HI[7:0]`	RW	TSM bit field to control when TSM `RF_STATUS` asserts in the TX sequence
`RF_STATUS_TX_LO[7:0]`	RW	TSM bit field to control when TSM `RF_STATUS` de-asserts in the TX sequence
`TSM_RF_STATUS_OVRD_EN`	RW	TSM bit field to provide override enable for TSM `RF_STATUS` output
`TSM_RF_STATUS_OVRD`	RW	TSM bit field to provide override value for TSM `RF_STATUS` output
`COEX_SEL`	RW	`RADIO_MISC` (`COEX_CTRL` register) bit field to select whether the TSM outputs (`RF_ACTIVE`, `RF_STATUS`, `RF_PRIORITY`) or the output of the active link layer are input to the RFMC.

3.5.1.3 RF_PRIORITY behavioral control

The NB radio provides the `RF_PRIORITY[1:0]` outputs to indicate the radio access priority. TSM or the active link layers can generate this signal.

Note: *If the TSM is chosen,* `RF_PRIORITY[1]` *is always* ***0****.*

Table 8 describes register bits in the TSM and `RADIO_MISC` to enable and control `RF_PRIORITY`. Refer to the link layer chapters for information on their **PRIORITY** output.

Table 8. RF_PRIORITY behavioral control

Field	Type	Description
`RF_PRIORITY_RX_HI[7:0]`	RW	TSM bit field to control when TSM `RF_PRIORITY` asserts in the RX sequence
`RF_PRIORITY_RX_LO[7:0]`	RW	TSM bit field to control when TSM `RF_PRIORITY` de-asserts in the RX sequence
`RF_PRIORITY_TX_HI[7:0]`	RW	TSM bit field to control when TSM `RF_PRIORITY` asserts in the TX sequence
`RF_PRIORITY_TX_LO[7:0]`	RW	TSM bit field to control when TSM `RF_PRIORITY` de-asserts in the TX sequence
`TSM_RF_STATUS_OVRD_EN`	RW	TSM bit field to provide override enable for TSM `RF_PRIORITY` output
`TSM_RF_STATUS_OVRD`	RW	TSM bit field to provide override value for TSM `RF_PRIORITY` output

Table 8. RF_PRIORITY behavioral control...*continued*

Field	Type	Description
COEX_SEL	RW	RADIO_MISC (COEX_CTRL register) bit field to select whether the TSM outputs (RF_ACTIVE, RF_STATUS, RF_PRIORITY) or the output of the active link layer are input to the RFMC.

3.6 Radio coexistence/FEM/LANT connections

Radio provides flexible mux configuration for four coexistence outputs, four FEM control outputs, and four localization outputs. Figure 11 show the detailed connections.

Note: *For the Bluetooth LE use case with NBU: Once asserted, the* `bt_grant_n` *input must remain asserted until 10 µs after the* `bt_request` *has been de-asserted.*

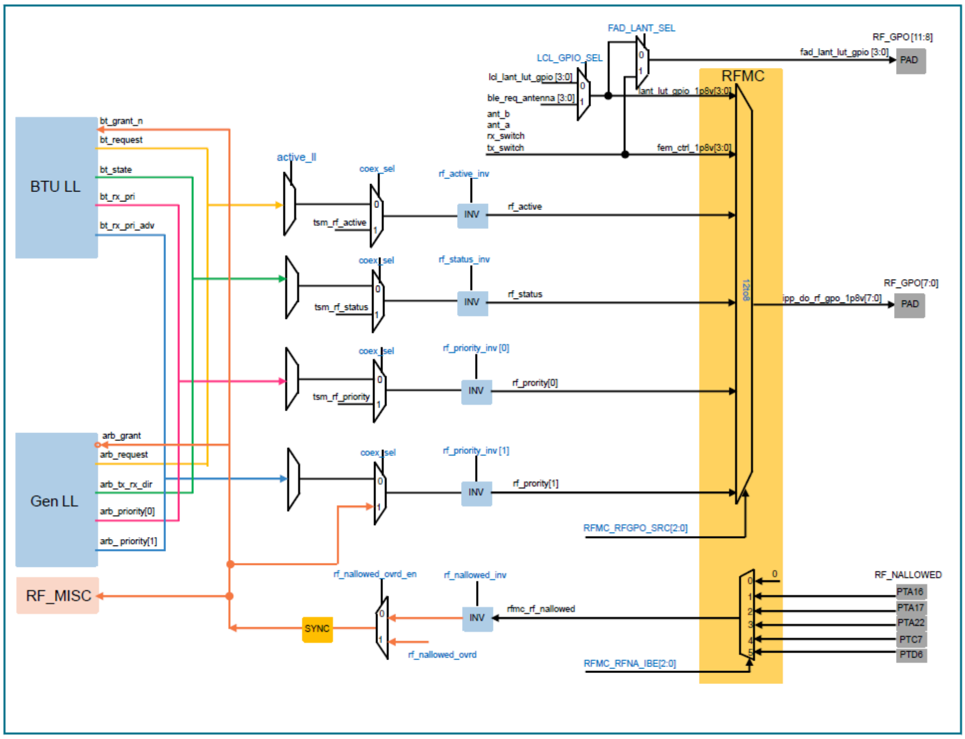

Figure 11. Radio Coexistence/FEM/LANT Mux diagram

For more details, see **Chapter 56.3.4.7 Radio Coexistence/FEM/LANT Connections** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.7 TSM RF_ACTIVE extension

The `TSM RF_ACTIVE` can be used as the **RF_ACTIVE coexistence** output of Radio. As such, this signal must be asserted high a programmable amount of time before a radio event takes place and remain high until the radio event is completed or aborted. There must not be glitches/unwanted transitions between successive radio events (for example, RX -> TX or TX -> RX). This case can be a problem for protocols, such as, Bluetooth LE which requires the transmission of an acknowledge packet shortly after reception and reception of an acknowledge packet shortly after transmission. Bluetooth LE advertising and scan states offer other scenarios where closely spaced (but not adjoining) TX and RX operations are required. The inter-frame spacing between the successive RX and

TX operations is long enough, so TSM RF_ACTIVE de-asserts and re-asserts between operations. Do not create unwanted transitions.

To remedy this case, a feature is added to TSM. It allows the TSM RF_ACTIVE output to be optionally extended by a programmable amount, after the nominal TSM sequence completes. The TSM RF_ACTIVE extension occurs for all sequences (TX and RX) for which TSM RF_ACTIVE is programmed to assert, whenever register TSM_SPARE1_EXTEND > 0.

Figure 12 shows the hardware mechanism for extending TSM RF_ACTIVE.

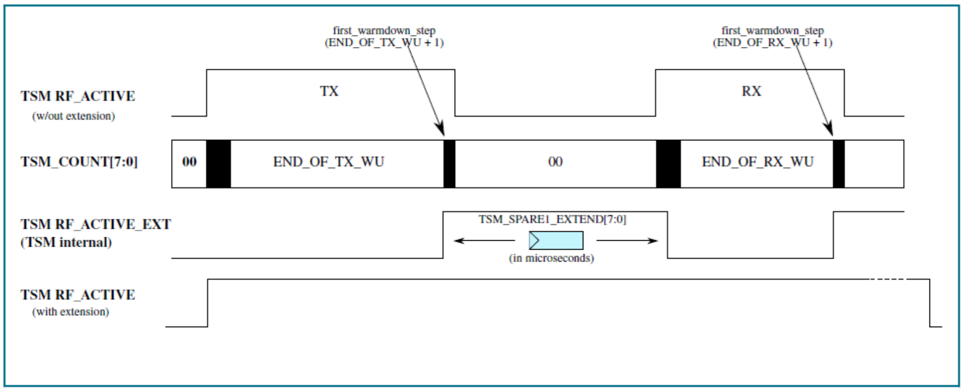

Figure 12. TSM RF_ACTIVE extension

The trigger for the extension is the first warm-down step (END_OF_xx_WU + 1) of TSM. It is reached whenever the Link Layer de-asserts its TX/RX command. If enabled, the extension signal asserts (high) and remains high for TSM_SPARE1_EXTEND microseconds. The extension signal (TSM RF_ACTIVE_EXT) is logically **OR-ed** with the existing TSM-controlled output TSM RF_ACTIVE, to generate the composite, extended RF_ACTIVE signal. Software can cut short the extension at any time by writing TSM_SPARE1_EXTEND=0. Setting this register to **0** also disables the extension feature from activating on any new TSM sequence. The register TSM_SPARE1_EXTEND[7:0] yields an extension range from 0 to 255 µs.

For more details, see **Chapter 56.3.5.6.2.10 TSM RF_Active Extension** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.8 Radio coexistence

The 2.4 GHz radio implements external IO signals to support coexistence with an external RF device operating within the same frequency band. The RFMC provides mux control (via RF_GPO[7:0] output of RFMC) for the coexistence outputs {RF_ACTIVE, RF_STATUS, and RF_PRIORITY[1:0]} from the 2.4 GHz radio. It provides additional control for the F_ACTIVE signal and the RF_NOT_ALLOWED coexistence input. The next few paragraphs discuss RFMC control of the RF_NOT_ALLOWED and RF_ACTIVE signals.

For more information on coexistence, see **Coexistence Interface** and **Coexistence/ FEM/LANT connections** in *KW45B41Z reference manual* (document KW45B41ZRM).

For RF_NOT_ALLOWED, the RFMC provides programmable control (RF*_COEXT[RFNA_IE] bit field) so that this coexistence signal can be sourced from any of the five device pins, or disabled.

Table 9. Wi-Fi coexistence function

Wi-Fi coexistence function	Pin direction	Pin description
RF_ACTIVE (REQUEST)	O	An output which is asserted prior to any Radio event and remains asserted during the event.
RF_STATUS (DIRECTION)	O	An output which indicates when the Radio is in an RX or TX even, software can also control this signal directly.
RF_PRIORITY	O	An output which indicates to the external Wi-Fi device that the radio event is a high priority and it needs access to the 2.4 GHz antenna.
RF_NOT_ALLOWED (! GRANT)	I	External signal which causes the internal Radio to crease radio activity.
RF_TX_CONF	I	Signal from an external Radio which indicates the availability of the 2.4 GHz antenna to the internal radio. **Note:** *This signal is not connected to the radio hardware. Radio software can use any interrupt-capable GPIO which the application assigns for this function.*

For RF_ACTIVE, the RFMC provides programmable control (RF*_COEXT[RFACT_SRC] bit field) to select whether this coexistence output is sourced by the RFMC, the Bluetooth LE bt_clk_req signal, or a mux of the RF_ACTIVE signal of TSM and the REQUEST signal of the active link layer. If RF_ACTIVE is sourced by the RFMC (RF*_COEXT[RFACT_SRC] = 00), this signal relies on the low-power controllers (one must be enabled) of RFMC. In this configuration, the RF_ACTIVE behavior is as follows:

- If RF*_COEXT[RFACT_IDIS] = 0
  - Asserts during the wake-up sequence of RFMC low-power controller, RF*_COEXT[RFACT_WKUP_DLY] 32 kHz clock cycles after the XO is enabled.
  - De-asserts when the RFMC low-power controller requests that the radio enters a low-power mode.
  - Software can cause RF_ACTIVE to be asserted during a low-power mode by setting the RF*_COEXT[RFACT_EN] bit field.
- If RF*_COEXT[RFACT_IDIS] = 1
  - Asserts when the TSM is busy.
  - De-asserts when the TSM is idle.

The QUIET_REQ outputs are related to RF_ACTIVE. When the radios are active, they are used inside the SOC to suppress SOC Core flash and/or RF Core flash activity if needed. These outputs have configurable behavior using QREQ_SRC, QREQ_SOC_EN, and QREQ_RF_EN bits of the RF*_COEXT register.

For more details, see **Chapter 56.2.5.3 Radio Coexistence** in *KW45B41Z reference manual* (document KW45B41ZRM).

3.8.1 RF Mode Controller (RFMC)

The Radio Mode Controller (RFMC) is responsible for sequencing the power mode of the 2.4 GHz radio domain and controlling the radio crystal oscillator (XO). Specifically, it supports the following features:

- Support for Deep Sleep and Power Down modes.

- Low-power mode entry/exit for the 2.4 GHz radio power domain.
- Enable of XO supported from both internal and external sources.
- ***Support for external coexistence interface for 2.4 GHz frequency band***
- 32 kHz timer to control low-power entry/exit times via Wake on Radio (WOR) or Manual (MAN) counters.
- Timer offsets to ensure XO and radio power restored prior to WOR/MAN exit event.
- Interrupts supported for XO and low-power radio wake-up events.

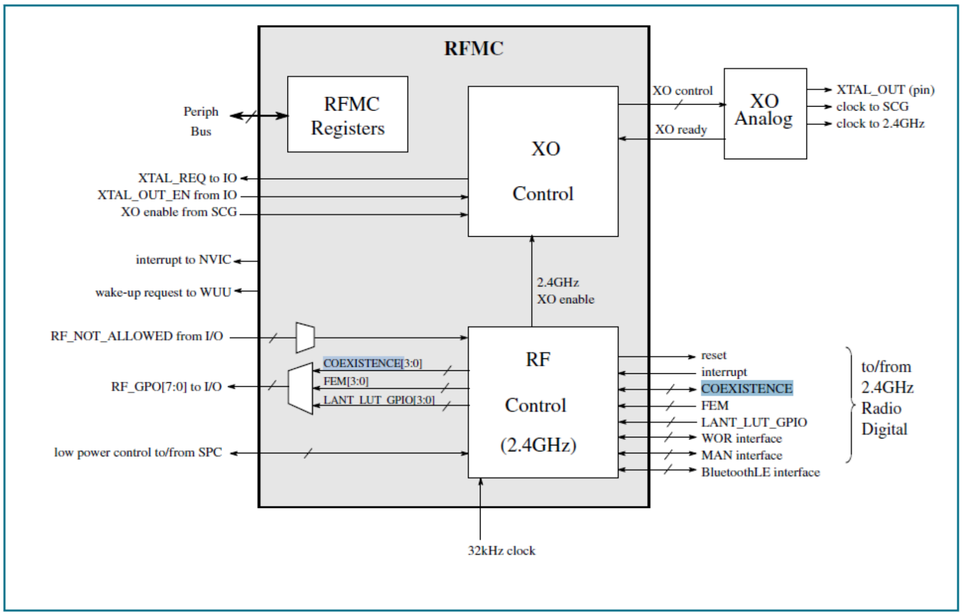

Figure 13. RFMC block diagram

For more details, see **Chapter 56.2.1 RFMC** in *KW45B41Z reference manual* (document KW45B41ZRM).

4 ANNEX

4.1 Wi-Fi ARB pattern

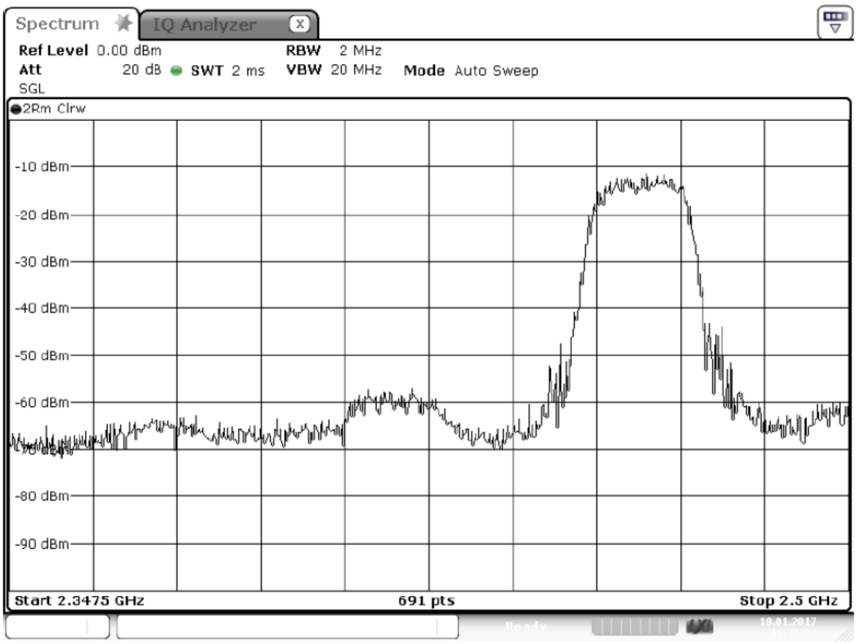

Figure 14. Original Wi-Fi stream (with side bands)

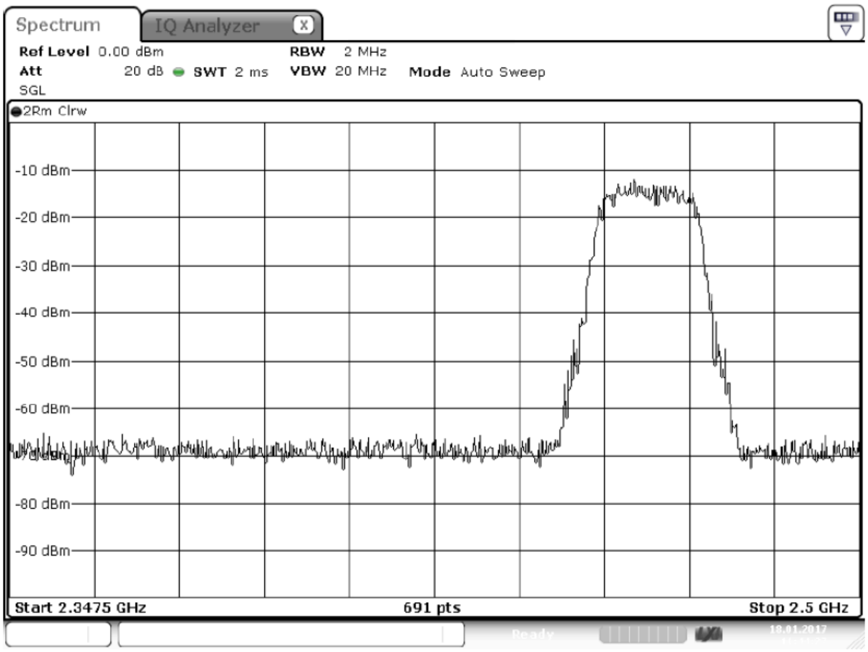

Figure 15. Wi-Fi once sampled and replayed with ARB generator

5 Revision history

Rev.	Date	Description
0	10 March 2022	Initial release

6 Legal information

6.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

6.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Contents

Date of release: 10 March 2022
Document identifier: AN13512